NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

BRIDGING OPERATIONAL AND STRATEGIC COMMUNICATIONS: INTEGRATING SMALL UNMANNED AIRCRAFT SYSTEMS AS AIRBORNE RELAY COMMUNICATION VERTICAL NODES

by

Jose D. Menjivar

September 2012

Thesis Advisor:	Douglas J. MacKinnon
Second Reader:	John H. Gibson

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2012	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE Bridging Operational and Strategic Communication Architectures: Integrating Small Unmanned Aircraft Systems As Airborne Tactical Communication Vertical Nodes	**5. FUNDING NUMBERS**
6. AUTHOR(S) Jose D. Menjivar	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ______N/A______.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release, distribution is unlimited	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The United States Department of Defense enterprise communication architectures are presently designed to support large-scale fixed organizations and rely primarily on satellite mediums. However, they are inadequate in tactical level environments, and are not readily available nor affordable to support multiple operators in various tactical locations. Incorporating Small-Unmanned Aircraft Systems (UAS) with communication repeaters could expand local mobile ad-hoc networks coverage for users in communications degraded environments and reduce satellite dependency. The proof of concept is focused on leveraging existing Government Off The Shelf (GOTS) technology with ever increasing Small-UAS functionality to explore the potential reduction of communication inadequacies in tactical environments. Through the efforts of this thesis, the goal is to extend and enhance beyond line of sight (BLOS) and on-the-move communications at the small unit level. The findings provide face validation that Small-UAS equipped with a communication payload can provide these services that enhance voice transmissions, and thus, enable TCP/IP data transfer in communication degraded environments without interfering with the Small-UAS primary ISR function or airworthiness. Future efforts in this line of inquiry may also inform the use of multiple Small-UAS to extend the networks and autonomous operations, and perhaps, eliminate the requirement for a ground Small-UAS operator.

14. SUBJECT TERMS Airborne Relay, Small-Unmanned Aerial System, UAV, SUAS, RQ-11B Raven, Wave Relay Quad Radio	**15. NUMBER OF PAGES** 159
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

BRIDGING OPERATIONAL AND STRATEGIC COMMUNICATION ARCHITECTURES: INTEGRATING SMALL UNMANNED AIRCRAFT SYSTEMS AS AIRBORNE TACTICAL RELAY COMMUNICATION VERTICAL NODES

Jose D. Menjivar
Major, United States Marine Corps
B.S., Syracuse University, 1998

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2012

Author: Jose D. Menjivar

Approved by: Douglas J. MacKinnon, PhD
Thesis Advisor

John H. Gibson
Second Reader

Dan C. Boger, PhD
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The United States Department of Defense enterprise communication architectures are presently designed to support large-scale fixed organizations and rely primarily on satellite mediums. However, they are inadequate in tactical level environments, and are not readily available nor affordable to support multiple operators in various tactical locations. Incorporating Small-Unmanned Aircraft Systems (UAS) with communication repeaters could expand local mobile ad-hoc networks coverage for users in communications degraded environments and reduce satellite dependency. The proof of concept is focused on leveraging existing Government Off The Shelf (GOTS) technology with ever increasing Small-UAS functionality to explore the potential reduction of communication inadequacies in tactical environments. Through the efforts of this thesis, the goal is to extend and enhance beyond line of sight (BLOS) and on-the-move communications at the small unit level. The findings provide face validation that Small-UAS equipped with a communication payload can provide these services that enhance voice transmissions, and thus, enable TCP/IP data transfer in communication degraded environments without interfering with the Small-UAS primary ISR function or airworthiness. Future efforts in this line of inquiry may also inform the use of multiple Small-UAS to extend the networks and autonomous operations, and perhaps, eliminate the requirement for a ground Small-UAS operator.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
- **A. THE PROBLEM 1**
- **B. THESIS OBJECTIVES 3**
- **C. THESIS STRUCTURE 4**

II. PRESENT TACTICAL MILITARY COMMUNICATION SYSTEMS AND UNMANNED AIRCRAFT SYSTEMS 7
- **A. INTRODUCTION 7**
- **B. TACTICAL MILITARY COMMUNICATIONS SYSTEMS 8**
  - **1. USMC Tactical Radio Systems 10**
  - **2. USMC Tactical Data Network Radios 17**
- **C. AIRBORNE RELAYS 19**
  - **1. Airships 20**
- **D. UNMANNED AIRCRAFT SYSTEMS 22**
  - **1. USMC Unmanned Aircraft Systems 24**
- **E. COMMERCIAL OF THE SHELF TECHNOLOGY 28**
- **F. SUMMARY 28**

III. TECHNOLOGICAL BACKGROUND 31
- **A. INTRODUCTION 31**
- **B. PREVIOUS EFFORTS 33**
  - **1. Dragon Warrior Communication Relay Testing 34**
    - ***a. Airborne Relay Configuration 34***
  - **2. Extension of Wireless Mesh Networks via RC VTOL UAV 36**
    - ***a. Wi-Fi Extension Via VTOL UAV Configuration 37***
- **C. SMALL-UAS TEST TECHNOLOGICAL BACKGROUND 38**
  - **1. Wireless Mesh Networks 38**
  - **2. Mobile Ad Hoc Networks 40**
  - **3. Communication Mobile Devices 40**
    - ***a. Wave Relay Quad Radio Router 40***
    - ***b. Wave Realy Single Board Module Payload 42***
    - ***c. Power Source 43***
- **D. UAS TEST PLATFORM 44**
  - **1. Aerovironment Raven RQ 11B 44**
  - **2. Network Performance Measuring Tool 46**
    - ***a. Transmission Control Protocol 46***
    - ***b. User Datagram Protocol 47***
- **E. SUMMARY 47**

IV. SMALL-UAS AIRBORNE RELAY TEST METHODOLOGY AND RESULTS 49
- **A. INTRODUCTION 49**
- **B. TESTING METHODOLOGY 50**
  - **1. Test Construct 50**

a. Test Distances ... *51*
b. Throughput ... *52*
C. TESTS AND RESULTS ... 52
1. Voice Transmission Test and Results ... 53
a. Baseline Voice Test ... *53*
b. Airborne Relay Node Voice Transmission Test ... *56*
c. Voice Transmission Observations ... *56*
2. Data Transfer Test and Results ... 57
a. Data Transfer Baseline ... *57*
b. Data Rate Baseline Test Observations ... *58*
c. Data Transfer Airborne Relay Node ... *59*
d. Airborne Relay Node Observations ... *59*
3. Comparison Models and Analysis ... 60
4. Small-UAS Network Node Operations ... 63
D. SUMMARY ... 63

V. CONCLUSIONS AND FUTURE RESEARCH ... 65
A. CONCLUSIONS ... 65
1. Communication Payload ... 65
2. Small-UAS Airborne Relay ... 65
B. FUTURE RESEARCH ... 66

APPENDIX A. TEST AND DEMONSTRATION PRELIMINARY WORK ... 69

APPENDIX B. WAVE RELAY™ QUAD RADIO ROUTER AND MANET DATA LINK DATA SHEETS ... 87

APPENDIX C. WAVE RELAY™ USER MANUAL ... 91

APPENDIX D. RAVEN RQ 11B DATA SHEET ... 123

APPENDIX E. IPREF BASELINE AND AIRBORNE RELAY TEST THROUGHPUT RATE AVERAGES ... 125

LIST OF REFERENCES ... 137

INITIAL DISTRIBUTION LIST ... 141

LIST OF FIGURES

Figure 1. Small-UAS Tactical Communication Relay Diagram 3
Figure 2. Metcalf's Law: Power of the Network is "Nodes-Squared" 7
Figure 3. Artist's Concept of U.S. Missile Defense Agency Prototype by Lockheed Martin (From: Jamison, 2005, p. 10). 21
Figure 4. 13th Marine Expeditionary Unit fields Combat SkySat Communications Relay Balloon (From: Barker, 2008). 22
Figure 5. USMC UAS Categories and Command Tier Levels (From: Isherwood, 2008). 26
Figure 6. Marine Expeditionary Force Task Organization, MCRP-5-12D (From: United States Marine Corps, 1998, pp. 2–3)..33
Figure 7. Dragon Warrior Test Communication Relay Payload (From: Tate, 2003, p. 4). 35
Figure 8. Dragon Warrior Test UAV, KAMAN K-MAX (From: Tate, 2003, p. 5). 36
Figure 9. Mikado Logo 24 RC Helicopter equipped with Mesh Dynamics 4000 Wi-Fi Wireless Access Point (From: Richerson, 2007, p. 35)..............................38
Figure 10. Wireless Mesh Network Consisting of Five Nodes, Introduction to Wireless Mesh Networks (From: Held, 2005, p. 6)..39
Figure 11. Wave Relay® Quad Radio Specification Diagram, Persistent Systems (From: Persistent Systems, n.d.). 41
Figure 12. Wave Relay™ Single Board Radio Module Small-UAS Payload 43
Figure 13. Thunder Power 2250mAh 3-Cell Rechargeable Battery Pack 43
Figure 14. AeroVironment Raven 11B UAS System (From: AeroViroment Inc., n.d.)...45
Figure 15. Google Earth™ Satellite Image of Baseline Test Area (From: Google Inc., 2012). 54
Figure 16. Wave Relay™ Quad Radio Graphic Settings Interface..................................55
Figure 17. *Iperf/JPerf* Network Performance Tool Baseline Throughput Rate Test 58
Figure 18. 1 Km TCP Null Hypothesis Computation and Excel Produced Results for Additional Distance and UDP Tests 61
Figure 19. TCP Data Throughput Rate Comparisons Between Baseline Test and Airborne Relay Node Test 62
Figure 20. TCP Data Throughput Rate Comparisons Between Baseline Test and Airborne Relay Node Test 62

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. USMC Tactical Communication Radios (From: Marine Corps Systems Command, 2011)....16
Table 2. USMC Tactical Data Radios (From: Marine Corps Systems Command, 2011). 19
Table 3. Unmanned Systems Associated with Net-Centric Architecture, FY2009–2034 Unmanned Systems Integrated Roadmap (From: Department of Defense, 2009, p. 15). 23
Table 4. Joint UAS Categories Aligned to FAA Regulations, FY2009–2034 Unmanned Systems Integrated Roadmap (From: Department of Defense, 2009, p. 95). 24
Table 5. Joint UAS Center of Excellence UAS Category Definitions, FY2009–2034 Unmanned Systems Integrated Roadmap (From: Department of Defense, 2009, p. 96). 24
Table 6. USMC UAS Programs of Record, FY2009–2034 Unmanned Systems Integrated Roadmap (From: Department of Defense, 2009, pp. 69–76). 27
Table 7. Wave Relay™ Quad Radio Router Technical Specifications, Persistent Systems (From: Persistent Systems, n.d.). 42
Table 8. AeroVironment Raven RQ 11B Technical Specifications (From: AeroViroment Inc., n.d.). 45
Table 9. Airborne Relay Node TCP & UDP Effectiveness Comparison Model 51
Table 10. Airborne Relay Node Voice Transmission Effectiveness Comparison Model 51
Table 11. Baseline Test Voice Transmission Results 55
Table 12. Measures of Effectiveness Voice Transmission Comparisons 56
Table 13. TCP and UDP Baseline Test Data Throughput Averages 58
Table 14. TCP and UDP Airborne Relay Data Throughput Averages 59

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AFATDS	Advanced Field Artillery Tactical Data System
ANGLICO	Air Naval Gunfire Liaison Company
AP	Access Point
ARG	Amphibious Ready Group
BLOS	Beyond Line of Sight
C2	Command and Control
CNR	Combat Net Radio
COE	Center of Excellence
COP	Common Operating Picture
COTS	Commercial of the Shelf
DAST	Distributed Applications Support Team
DC	Direct Current
DoD	Department of Defense
EMW	Expeditionary Maneuver Warfare
ENM	EPLRS Network Manager
EPLRS	Enhanced Position Location Reporting System
FAA	Federal Aviation Administration
FM	Frequency Modulation
GIG	Global Information Grid
GOTS	Government off the Shelf
GPS	Global Positioning System
HAA	High Altitude Airships
HAP	High Altitude Platforms
HF	High Frequency
ISR	Intelligence Surveillance Reconnaissance
JUAS	Joint Unmanned Aircraft System
LAN	Local Area Network
LOS	Line of Sight

MANET	Mobile Ad Hoc Network
MCRP	Marine Corp Reference Publication
MDA	Missile Defense Agency
MEF	Marine Expeditionary Force
MEU	Marine Expeditionary Unit
MOE	Measures of Effectiveness
MSL	Mean Sea Level
NCW	Network Centric Warfare
NLANR	National Laboratory for Applied Network Research
NPS	Naval Postgraduate School
PLRS	Position Location Reporting System
RC	Remote Control
RF	Radio Frequency
RoIP	Radio Over Internet Protocol
RS	Radio Sets
RSTA	Reconnaissance Strike and Target Acquisition
SATCOM	Satellite Communication
SINCGARS	Single Channel Ground Airborne Radio
Small-UAS	Small Unmanned Aircraft System
STOM	Ship-to-Object Maneuver
TCP/IP	Transmission Control Protocol/Internet Protocol
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UHF	Ultra High Frequency
USMC	United States Marine Corps
USN	United States Navy
VHF	Very High Frequency
VTOL	Vertical Takeoff and Landing
WLAN	Wireless Local Area Network
WWI	World War I
]WWII	World War II

ACKNOWLEDGMENTS

I would like to thank my wife Lisa, whose constant encouragement and moral support were the source of inspiration to pursue a thesis subject I was genuinely passionate about and potentially help others in the future. I would also like to thank the outstanding and professional United States Army soldiers at Camp Roberts, CA whose patience and enthusiasm allowed this project to come to fruition. I would also like to thank Mr. John H. Gibson whose mentorship and sincere belief in the project encouraged me not to waiver in times of difficulties. Lastly, I would like to thank the men and women who serve this great nation and know that this project is an effort to improve the quality of communications at the tactical level and empower those at the tip of the spear.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. THE PROBLEM

The introduction of Network Centric Warfare (NCW) has dramatically changed how today's military communicates. Technological advancements have provided armed forces the ability to leverage critical information at unprecedented rates and reliability. A contributing factor to these enhancements has been the development and expansion of global telecommunication infrastructure. Admiral Arthur Cebrowski has been called "the father of Network Centric Warfare," who had as a vision a force structure that was interconnected with interoperable systems, which meant composite systems produce a common operating picture for military commanders to make informed decisions. This vision also entailed the ability to share time sensitive information without any physical boundaries (Dombrowski & Gholz, 2006, p. 189). NCW did not revolve around a single piece of equipment, but rather on multiple nodes that enable transfer of information at incredible rates of speed. It also meant the ability to reduce the amount of personnel required on the ground during conflicts. The new force would be smarter and lighter equipped, with smart weapons that would minimize friendly attrition and collateral damage.

The NCW concept was tested and validated in the recent conflicts of Operation Enduring Freedom, Afghanistan, 2001 and again during Operation Iraqi Freedom, Iraq, 2003. During the conventional kinetic shaping of these two operations, NCW performed well. These shaping operations involved the use of smart weapons like Tomahawks and other precision guided missiles where sensors collected intelligence and passed information over high-speed enterprise level communication links. The large-scale command and control was seamlessly integrated; however, small ground units had a difficult time operating with dated communication equipment. Instances were experienced first hand during the 2003 invasion of Iraq in which convoys were separated due to a lack positive communication. In one particular case, the author and his unit, an artillery battery, had gone past the division's forward line of troops because of degraded communication. The unit was put at great risk, since they were behind enemy lines with

little firepower. The second order effects from this situation were a friendly fire incident when the battery responded to a fire mission and pointed their weapons into friendly positions. These examples are but a few that illustrate and highlight the importance for exceptional communication systems at the tactical level. The situations became more precarious, both in Afghanistan and Iraq, when the conflicts transitioned from symmetrical battlefields to asymmetrical battle spaces.

When the Afghanistan and Iraq conflicts phased into security and stability operations a requirement arose for foot soldiers to patrol communications-degraded environments and clear them of radical violent insurgents. These environments included vast expanses of deserts, urban built-up areas, and in the case of Afghanistan, mountainous terrain, which severely impacted the ability to communicate with the line of sight (LOS) tactical radios used by small units. Much like the commercial world, where challenges still exist in delivering communication services to users in remote and rural areas, and also referred to by the telecommunication industry as the "First and Last Mile," the armed forces struggle with providing equitable capabilities to tactical users operating in communications-degraded environments.

A solution introduced by both the commercial and military sectors to improve the "Last Mile" phenomena has been to increase satellite communication availability. However, the cost of satellite communication prohibits providing every field operator a dedicated channel. Further, such capabilities in some cases may limit the maneuverability or mobility of the Marines or soldiers being supported. Alternatives to cost-prohibitive satellite solutions include satellite-surrogates, such as high-altitude airships.

The high-altitude airships have yet to be widely adopted because of their susceptibility to atmospheric conditions when operating at 65,000 feet. The approximate cost of $50,000,000 per airship does not represent order-of-magnitude savings when compared to $200,000,000 per satellite (Jamison, 2005, p. 35). Such airships have not gained traction, and with budget cuts, may not be a viable tactical communication solution. However, the concept of airborne vertical nodes might be further explored and may prove to be cost effective when applied to existing military unmanned aircraft system platforms.

B. THESIS OBJECTIVES

The purpose of this study is to examine how scalable communication payloads and Small-UAS can significantly improve field communications in communications-degraded environments. The proof of concept seeks to demonstrate that the integration of airborne vertical nodes with mobile ad-hoc networks (MANET) could provide users beyond line of sight and persistent on-the-move communication capabilities. The premise behind the airborne vertical is to enable a small tactical unit the ability to communicate with higher and adjacent units in communication-degraded environments. The theory behind the proof of concept is that a small tactical unit outfitted with a hand launched, Small-UAS equipped with a communication payload can establish a hasty MANET in the most remote environments. The tactical unit would deploy the Small-UAS at an altitude that has cleared masking terrain, establish a link with neighboring nodes, and look to extend the networks coverage area. In convoy scenarios, the Small-UAS can be deployed to provide both ISR and communication links that enhance on the move persistent communications. Figure 1 is a simplified communication diagram that depicts the research goal.

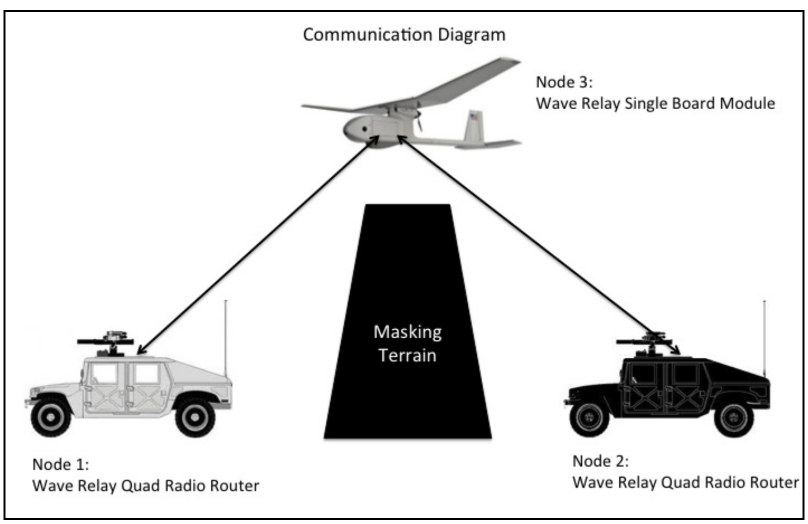


Figure 1. Small-UAS Tactical Communication Relay Diagram

The outcome is to verify use of airborne vertical nodes as communications platforms to mitigate current communication inadequacies by providing beyond line of sight (BLOS), persistent communications while on the move. In particular, the ability to provide consistent or predictable quality of service and increased higher data transfer rates compared to status quo capabilities, within a 4-kilometer area of operation is investigated. It is also the goal to reinforce the concept of utilizing UAS platforms to perform more than a single mission while airborne to promote cost efficiency and mitigate inadequacies in field communications.

C. THESIS STRUCTURE

Field tests were conducted to capture the following measure of effectiveness (MOEs), voice transmission quality and data transfer rates within predetermined distances of 1km, 2km, 3km, and 4km. The MOEs were determined by establishing a set baseline from test results and attempting to achieve similar performance with the airborne relay. However, the ultimate goal, regardless of throughput performance, was to validate that an airborne relay platform could enable communications where they previously did not exist.

The majority of the experiments were conducted in controlled environments with instruments that measure Transmission Control Protocol/Internet Protocol (TCP/IP) throughput rates for data transfers. However, during mature testing stages, experiments were conducted in less controlled environments using active duty military operators to mimic real world field scenarios. These experiments required the assistance of auxiliary military operators employing organic communication equipment linked and unlinked to the airborne vertical nodes, which validated communication performance improvements in the degraded environments.

The research and findings are organized in the following manner. Chapter II provides a background and literature review. This chapter discusses the current inadequacies in tactical field communications in remote and austere areas encompassing a 4-kilometer radius. This chapter also presents the challenges faced by field operators while attempting to coordinate and communicate beyond line of sight and while on-the-

move, both on foot and mounted in vehicles. This chapter also examined past and present military communication equipment, with a special focus on the United States Marines Corps (USMC). Also reviewed were USMC unmanned aerials systems, how they are employed, and how they fit into organizations' command and control constructs.

Chapter III examines the Marine Corps organizational structure and the need to improve communication infrastructure at the tactical level. Also discussed are previous work in the area of airborne relay communications, prior to attempts to gain interest and adaptation of the airborne relay concept. This chapter also provides a detailed technical background on the equipment used to perform the tests and demonstrations.

Chapter IV describes the testing methodology and test constructs, and the preliminary actions prior to creating a formal test environment. The baseline test results for both voice and data transmissions are discussed, and how they provide target goals for the airborne relay tests. This chapter also provides analysis of the data collected during the experimentation and validates that the airborne relay can enable BLOS and persistent on-the-move communications in communications-degraded environments.

Chapter V summarizes the findings from baseline tests and field tests and demonstrations. It also describes future research opportunities in the application of mobile ad-hoc networks in communications-degraded environments and the integration of GOTS communication technology and existing UAS platforms.

THIS PAGE INTENTIONALLY LEFT BLANK

II. PRESENT TACTICAL MILITARY COMMUNICATION SYSTEMS AND UNMANNED AIRCRAFT SYSTEMS

A. INTRODUCTION

NCW operations delivered the U.S. military powerful tools to achieve information superiority over adversaries in the recent Global War On Terrorism, both in Operation Enduring Freedom, in Afghanistan, and Operation Iraqi Freedom, in Iraq. NCW provided commanders at the strategic level with critical elements for detailed understanding of competitive battlespace and time. At the operational level, NCW has given commanders a close linkage among units, interactions, and the operating environment. At the tactical level, NCW operations provided commanders with timely access to critical information.

The NCW architecture is based on three critical elements: sensor grids, transaction (engagement) grids, and information grids hosted by a high-quality information backplane (Cebrowski, 1998, p. 5). The NCW concept creates an interconnected set of nodes across the battlespace that communicates with each other or serves as relays and passes valued information to other nodes. The NCW theory exploits the tenet of Metcalfe's Law, which states, "connect any n of machines and you get n^2 potential value" (Gilder, 1993, p. 1).

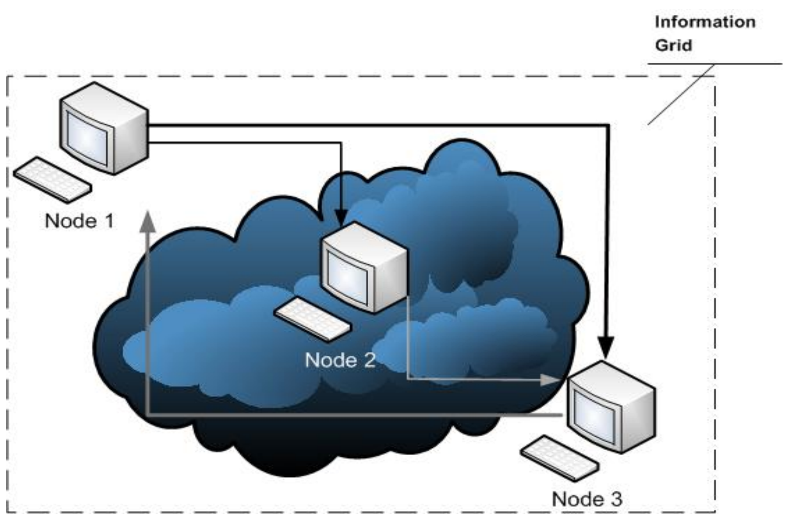


Figure 2. Metcalf's Law: Power of the Network is "Nodes-Squared"

The NCW network incorporates nodes that include computers, routers, switches, satellites, telephones, and tactical radios. The theory of NCW operations is that by increasing the amount of nodes, a non-linear increase in valued-information sharing occurs. Cebrowski's states:

> Network-Centric Warfare derives its power from the strong networking of a well-informed but geographically dispersed force. The enabling elements are a high-performance information grid, access to all appropriate information sources, weapons reach and maneuver with precision and speed of response, value-adding command-and-control (C2) processes to include high-speed automated assignment of resources to need and integrated sensor grids closely coupled in time to shooters and C2 processes. (Cebrowski, 1998, p. 12)

The outcome of the information grid concept has been the development and implementation of the Global Information Grid (GIG.) The GIG has enabled American forces the ability to leverage the delivery of critical information at unprecedented transfer rates covering vast geographical distances. The sensor grid, transaction grid, and GIG are able to communicate using an assortment of communication components. These components range from commercial-off-the-shelf (COTS) technologies to communication equipment specifically designed and manufactured for military use.

B. TACTICAL MILITARY COMMUNICATIONS SYSTEMS

The advent of U.S. military electronic communication networks can be traced to the introduction of the telegraph in the 19th century, which forever changed how military commanders would command and control forces on the battlefield. The first American use of electrical telegraphy dates back to the American Civil War, where both the U.S. Army Signal Corps and the Confederate Signal Corps used it to command and control forces. During this time period, the telephone had also gained great popularity in the civilian sector and staff officers began demanding telephones to expedite the receipt and delivery of orders (Ryan, 2002, p. 111).

The telegraph is referenced as a revolutionary technology that was the catalyst for modern communication innovations. However, new innovations come with a set of complexities and implementation challenges; in the case of telegraphy, it was the amount

of logistics associated with fixed cables and the process of laying wire underground to form grids that would ensure communication with all subordinate commanders. The use of wired communications networks were effective in fixed, static positions in which troops remained fairly non-mobile and their movements were slight, such as trench warfare tactics used during World War I.

In World War I, the tank was introduced; however, in World War II, tanks gained a larger role on the battlefield because trench warfare was no longer used. In other words, mobility and the expansion of the battlefield had grown by orders of magnitude and created a communication dilemma because it was not feasible to lay wire throughout a vast battlefield to maintain positive command and control of forces that were moving at a high rate. The development of Frequency Modulation (FM) radio would alleviate the need for wire and provide the U.S. military forces with noise-free communications, C2 of highly mobile forces, coverage of large areas, and man-portable radios for infantry units that were widely dispersed across the battlefield (Ryan, 2002, p. 113).

The introduction of the FM radio not only enhanced the U.S. Military C2 capabilities during World War II, but it set the path for the development of the current U.S. military's communication doctrine that entails two distinct battlefield communication systems. The first type, above the battalion level, is known as trunk communications that are designed to create high capacity links between supported units and headquarters. These links were point-to-point and limited to connecting to one unit at a time; an example of duplex communication is the telephone. The second type is used at the battalion and below for tactical operations, and is referred to as single channel radio or combat net radio (CNR.) The links are established using single frequency, half-duplex, all-informed (broadcast) radio nets (Ryan, 2002, p. 114), which allows commanders to address numerous units simultaneously and avoid the need to address each individually, and as such, reduce time and repetition.

The two broad U.S. military communication services have evolved into two subsystems integrated into most recent telecommunications technology.

The subsystems are categorized as CNR and Trunk communication subsystems:

> CNR subsystem is a ruggedized, portable radio (HF, VHF and UHF) network carried as an organic communications system for combat troops (brigade level and below.) Radios are invariably interconnected to form single-frequency, half-duplex, all-informed, hierarchical nets, providing tactical commanders with effective support to command and control. (Ryan, 2002, p. 115)
>
> Trunk communications subsystem provides high-capacity communications links down to brigade level. The subsystem traditionally comprises multichannel radio equipment, line, switches, and terminating facilities to provide voice, telegraph, facsimile, and data communications, as well as a messenger service. (Ryan, 2002, p. 115)

These subsystems form the foundation of the current U.S. military communication systems, as well as the initial framework of the NCW concept. Each service has diligently embarked in developing specific technological solutions to integrate with NCW operations and each continues to concurrently develop and procure equipment that meets their respective mission sets. In the case of the United Sates Marine Corps, its mission is to be "America's Expeditionary Force in Readiness" (United States Marine Corps, 2011, p. 3). This broad mission statement encompasses several responsibilities the Marine Corps has to meet, which are separated into five core capabilities: conduct military engagement, respond to crises, project power, conduct littoral maneuver, and, lastly, counter irregular threats " (United States Marine Corps, 2011, p. 3). The Marine Corps is a maritime service and the majority of its assigned missions are conducted in concert with the United States Navy amphibious fleet. However, the Marine Corps will also phase ashore and integrate with joint, coalition, and allied forces during humanitarian or military engagements requiring U.S. intervention. The Marine Corps' various missions require a diverse suite of communication equipment that will meet the challenges of ship-to-shore operations, and, once ashore, networks that will enable commanders to conduct C2 of ground, air, and logistic units over large geographical areas.

1. USMC Tactical Radio Systems

The Marine Corps' diverse missions require communication systems that support operations and maneuver from air, land, and sea. At the small tactical unit levels

(battalion and below), Marines require highly mobile communication systems; not only does the user require mobility, but the network also needs to be as mobile as the user. In commercial wireless communication systems, such as cellular or "WiFI hotspots," the user is the mobile piece of the equation; the user moves about and connects to fixed infrastructures that create links between nodes. However, in military applications, the networks must be as flexible and mobile as the user and must be transportable to enable the communication links required in environments in which no infrastructure exists, or in which the host nation infrastructure use is restricted or has security vulnerabilities. To address these challenges, the military developed transportable networks known as *Mobile Network Infrastructure*, which is part of the CNR communications subsystem. The mobility of these networks is achieved by mounting radio systems onto vehicles and man-packs that serve as both terminals and network nodes.

CNR subsystems have proven to be an effective means of military units communicating on the move. While voice is the primary means of communication, however, modern robust radios also provide the ability to transmit limited amounts of data files containing text, picture, or video. Nonetheless, despite the technological advancements made to end–terminals, CNR's greatest disadvantage is that it is limited by terrain: CNR radios must be within line-of-sight to communicate.

During the last decade, the Marine Corps has acquired various CNR subsystem radios compatible with transportable mobile network infrastructure that provide the mobility to support both its maritime Marine Expeditionary Unit mission and combat military engagements in Afghanistan and Iraq. Marine forces equipped with these radios gain flexibility through features, such as single frequency, half-duplex, all-informed ("broadcast") communications that allow for better C2 on dispersed battlefields and ship-to-shore operations (Ryan, 2002, p. 169). Table 1 is a comprehensive list of the current USMC CNR radios in use in combat operations in Afghanistan, Marine Expeditionary Units, and special contingency Marine task forces.

Command and Control Radios			
High Frequency Man-pack Radio, AN/PRC-150	**System Characteristics**	**Description**	**Locations**
	***Tech:*** Digital ***Spectrum:*** HF-VHF 1.6MHz – 60MHz ***Orientation:*** Omni-directional ***Mobility:*** OTM ***Power:*** Medium-20 Watts ***Operational Mode:*** Voice, Low Data Rate 9600Kbps ***Distance:*** 30+Miles ***Encryption:*** Embedded NSA Type 1	The AN/PRC-150 provides half duplex HF and VHF tactical radio communications. It provides voice or data (using a modem) through Single Sideband modulation selectable for either USB or LSB. The AN/PRC-150 is capable of ALE compatible with MILSTD-188-141A ALE for frequency analysis.	***CE:*** Comm Bn, Force Recon, ANGLICO ***GCE:*** HQ Bn, Inf Reg, Inf Bn, Recon Bn ***ACE:*** MACG ***LCE:*** MLG
High Frequency Vehicular Radio (HFVR), AN/MRC-148	**System Characteristics**	**Description**	**Locations**
	***Tech:*** Digital ***Spectrum:*** HF-VHF 1.6MHz – 60MHz ***Orientation:*** Omni-directional ***Mobility:*** OTM ***Power:*** High/low-150/60Watts ***Operational Mode:*** Voice, Data Rate 19.2Kbps ***Distance:*** BLOS ***Encryption:*** Embedded NSA Type 1	The AN/MRC-148 is a vehicular mounted, 150W variant of the AN/PRC-150 radio set. The AN/MRC-148 is virtually identical to the AN/VRC-104 but is distinguished by being a dedicated communication asset whose use is directed by the G6/S6.	***CE:*** Comm Bn, Force Recon, ANGLICO ***GCE:*** HQ Bn, Inf Reg, Inf Bn, Recon Bn ***ACE:*** MACG ***LCE:*** MLG
Multi-Band Radio (MBR), AN/PRC-117G	**System Characteristics**	**Description**	**Locations**
	***Tech:*** Digital ***Spectrum:*** 30 MHz-2 GHz Narrowband (NB): VHF Low 30-90 MHz VHF High: 90-225 MHz UHF Low: 225-512 MHz SATCOM UHF Low: 243-270 MHz and 292-318 MHz Wideband (WB): UHF: 225 MHz-2 GHz ***Orientation:*** Omni-directional ***Mobility:*** Man-pack ***Power:*** Selectable – NB: 10W, SATCOM: 20W, WB: 20W peak/5W average ***Operational Mode:*** Voice/Data (to 3.6Mbps) ***Distance:*** 300 meters to 35 Kilometers or LOS ***Encryption:*** Embedded Sierra II Based Type I COMSEC ***Data Capability:*** IP Capable and ANW2	The AN/PRC-117G MBR covers the entire 30 MHz to 2 GHz frequency range while offering embedded NSA Type- 1 COMSEC, SATCOM, Electronic Counter-countermeasures (ECCM) capabilities, and Embedded GRAM SAASM GPS. The AN/PRC-117G includes all waveforms offered by the AN/PRC-117F and is interoperable with the current radio inventory. The added ANW2 waveform provides OTM networking of high-bandwidth voice, video and data; currently approved for home stations training and OEF.	***CE:*** TBD ***GCE:*** Inf Bn ***ACE:*** TBD ***LCE:*** TBD

Multi-Band Radio (MBR), AN/PRC-117F (V)1(C)	**System Characteristics**	**Description**	**Locations**
	***Tech:*** Digital ***Spectrum:*** VHF Low 30-90 MHz,VHF/VHF-AM 116-150 225-400 MHz,UHF SATCOM, 243-270 MHz, 292-318 MHz, VHF/UHF 30-512 MHz ***Orientation:*** Omni-directional ***Mobility:*** Man-pack to vehicular configuration ***Power:*** Selectable - 1, 5, or 20 watts ***Operational Mode:*** Voice/Data (to 64Kbps) ***Distance:*** 300 meters to 35 Kilometers or LOS ***Encryption*** Embedded Type I, ANDVT COMSEC ***Data Capability:*** IP Capable	The AN/PRC-117F MBR covers the entire 30 to 512 MHz frequency range while offering embedded COMSEC, SATCOM, and ECCM capabilities. The AN/PRC-117F provides secure interoperability with SINCGARS and a host of other tactical radios.	***CE:*** ANGLICO, CBIRF, CIHEP, Comm Bn ***GCE:*** Recon Bn, Comm Co, Inf Bn ***ACE:*** Comm Sqdn ***LCE:*** CCSS, Comm CO
Multi-Band Vehicle Radio (MBVR), AN/VRC-103(V)2	**System Characteristics**	**Description**	**Locations**
	***Tech:*** Digital ***Spectrum:*** VHF Low 30-90 MHz,VHF/VHF-AM 116-150 225-400 MHz, UHF SATCOM,243-270 MHz, 292-318 MHz, VHF/UHF 30-512 MHz. ***Orientation:*** Omni-directional ***Mobility:*** Man-pack to vehicular configuration ***Power:*** Selectable - 1, 5, 20 or 50 watts ***Operational Mode:*** Voice/Data (to 64Kbps) ***Distance:*** 300 meters to 35 Kilometers or LOS ***Encryption*** Embedded Type I, ANDVT COMSEC	The AN/VRC-103(V)2 is a vehicular mounted, 50 watt capable variant of the AN/PRC-117F MBR radio. The VRC- 103(V)2 MBR covers the entire 30 to 512 MHz frequency range while offering embedded COMSEC, SATCOM, and ECCM capabilities.	***CE:*** ANGLICO, CBIRF, CIHEP, Comm Bn ***GCE:*** Recon Bn, Comm Co, Inf Bn ***ACE:*** N/A ***LCE:*** CCSS, Comm CO

Hand Held Radios			
Tactical Handheld Radio (THHR), AN/PRC-148	**System Characteristics**	**Description**	**Locations**
	***Urban/Maritime*** ***Tech:*** Digital ***Spectrum:*** VHF-UHF 30 MHz – 512 MHz ***Orientation:*** Omni-directional ***Mobility:*** Hand-held ***Power:*** Low – .1, .5, 1, 3, & 5 Watts ***Operational Mode:*** Voice/Data (to 64Kbps) ***Distance:*** LOS to 12 Miles ***Encryption***: Embedded NSA Approved Type I	The THHR is a standardized, lightweight, tactical, hand held radio that provides secure, multi-band communications in the 30-512 MHz (AM & FM) frequency spectrum.	***CE:*** MCSF Bn, MARSOC, MEU HQ, ANGLICO, CI/HumInt Co, RadBn ***GCE:*** Div, Arty Regt/Bn, Inf Regt/Bn, Sup Bn, AsltAmphib Bn, CbtAslt Bn, CbtEng Bn, LAR Bn, Recon Bn, Tank Bn ***ACE:*** Wing, MWCS, MACS, MAGs, MALS, LAAD Bn, VMU Sqdn ***LCE:*** MLG, H&S Bn, Sup Bn, TransSpt Bn, LdgSpt Bn
Dual Vehicle Adapter (DVA) AN/VRC-111	**System Characteristics**	**Description**	**Locations**
	***Tech:*** Digital ***Spectrum:*** AM-FM-VHF-UHF 30 MHz – 512 MHz ***Orientation:*** Omni-directional, Multiband ***Mobility:*** Vehicular and Handheld ***Power:*** Vehicular and Handheld ***Operational Mode:*** Voice, Retrans and Data w/Modem ***Distance:*** LOS to 12 Miles ***Encryption***: Embedded NSA Approved Type I	The AN/VRC-111 Dual Vehicle Adapter (DVA) is a standardized, Vehicular Radio Set Amplification Kit, that amplifies, and houses the AN/PRC-148 THHR. The AN/VRC 111 provides secure, multi-band communications in the 30-512 MHz (AM & FM) frequency spectrum.	***CE:*** MARSOC ***GCE:*** TBD ***ACE:*** TBD ***LCE:*** TBD

Tactical Handheld Radio (THHR), AN/PRC-152	**System Characteristics**	**Description**	**Locations**
	***Tech:*** Digital ***Spectrum:*** VHF-UHF 30 MHz – 512 MHz ***Orientation:*** Omni-directional ***Mobility:*** Hand-held ***Power:*** Low-.25,1,2,&5Watts ***Operational Mode:*** Voice, Low rate data (w/Modem) ***Distance:*** LOS to 12 Miles ***Encryption:*** Embedded NSA Approved Type I	The AN/PRC-152 is a standardized, lightweight, tactical, hand held radio that provides secure, multi-band communications in the 30-512 MHz (AM & FM) frequency spectrum. The system can be configured for handheld (AN/PRC-152) or vehicular (AN/VRC-110 and AN/VRC-112) applications.	***CE:*** Most Commands ***GCE:*** Most Commands ***ACE:*** Most Commands ***LCE:*** Most Commands
Dual Vehicle Adaptor (DVA) AN/VRC-110	**System Characteristics**	**Description**	**Locations**
	***Tech:*** Digital ***Spectrum:*** AM-FM-VHF-UHF 30 MHz – 512 MHz ***Orientation:*** Omni-directional, Multiband ***Mobility:*** Vehicular and Hand-held ***Power:*** Low-.25,1,2,&5Watts HH & High: 20 and 50 Watt VAA ***Operational Mode:*** Voice, Low rate data (w/Modem) ***Distance:*** LOS to 12 Miles ***Encryption:*** Embedded NSA Approved Type I	The AN/VRC-110 Dual Vehicle Adaptor (DVA) is a standardized, Vehicular Radio Set Amplification Kit, that amplifies, and houses the AN/PRC-152 THHR. The AN/PRC-152 provides secure, multi-band communications in the 30-512 MHz (AM & FM) frequency spectrum. The system can be configured for handheld or vehicular applications	***CE:*** Most Commands ***GCE:*** Most Commands ***ACE:*** Most Commands ***LCE:*** Most Commands
Single Vehicle Adapter (SVA) AN/VRC-112	**System Characteristics**	**Description**	**Locations**
	***Tech:*** Digital ***Spectrum:*** AM-FM-VHF-UHF 30 MHz – 512 MHz ***Orientation:*** Omni-directional, Multiband ***Mobility:*** Vehicular and Hand-held ***Power:*** Low-.25,1,2,&5Watts HH & High: 50 Watt VAA ***Operational Mode:*** Voice, Low rate data (w/Modem) ***Distance:*** LOS to 12 Miles ***Encryption:*** Embedded NSA Approved Type I	The AN/VRC-112 Single Vehicle Adaptor (SVA) is a standardized, Vehicular Radio Set Amplification Kit, that amplifies, and houses the AN/PRC-152 THHR. The AN/PRC-152 provides secure, multi-band communications in the 30-512 MHz (AM & FM) frequency spectrum. The system can be configured for handheld or vehicular applications.	***CE:*** Most Commands ***GCE:*** Most Commands ***ACE:*** Most Commands ***LCE:*** Most Commands

Integrated Intra-Squad Radio (IISR) , AN/PRC-153	System Characteristics	Description	Locations
	***Tech:*** Digital ***Spectrum:*** 380 MHz - 470 MHz UHF ***Orientation:*** Omni-directional ***Mobility:*** Hand-held ***Power:*** 5 Watts Variable ***Operational Mode:*** Voice ***Distance:*** 1Km ***Encryption:*** AES 256 bit	The IISR is an XTS-2500 representing a commercially and militarily proven solution that is technologically mature and stable. The IISR is a form, fit radio modified slightly for use by the Marine Corps. The two primary components for the IISR are the radio and Quiet-Pro tactical headset. The radio provides lightweight handheld tactical communications capability intended for short-range urban warfare, open terrain, and heavy vegetation environments. The IISR is capable of both analog and digital operations.	***CE:*** Most Commands ***GCE:*** Most Commands ***ACE:*** Most Commands ***LCE:*** Most Commands

Table 1. USMC Tactical Communication Radios (From: Marine Corps Systems Command, 2011).

These radios operate in various spectrums that include HF, VHF, UHF, and Satellite Communication (SATCOM.) The different frequency spectrums allow Marines to assemble communication suites best suited for each Marine unit and its particular function in tactical environments. SATCOM provides the greatest range of services, such as long-range communication, data file transfers, and persistent availability. However, due to cost constraints and resource availability, SATCOM channels are not available to every Marine tactical unit and operational prioritization will dictate what unit is assigned dedicated SATCOM channels. HF frequency radios still have specific utility in maritime environments; however, transmission rates linked to bandwidth and transmitter power make HF less capable for C2 in fast-paced dynamic environments. Marine combat forces, such as infantry, artillery, and armor units, depend on VHF and UFH radios to conduct most of their operations. These frequencies can be limited by terrain and restricted by line of sight between terminals. Relays must occur for units to communicate with each other.

The Marine Corps and its sister services have opted to procure COTS communications equipment to meet the demands of an asymmetrical battlefield and stay technically current as communication technology advances in orders of magnitude. This approach reduces the time it takes to design, develop and deploy critical equipment to the warfighter, as well as reducing acquisition program risks as COTS products are generally well-proven by the commercial user base. The use of COTS instead of the traditional

Department of Defense (DoD) acquisition methodology, in which the capability acquired includes extensive product design and development, offers commanders the flexibility to get critical equipment to the warfighter in a timely manner and maintain an edge over his adversary. At the tactical levels, COTS technology has been introduced via commercial laptops that allow soldiers and Marines to chat critical information over secure tactical networks.

2. USMC Tactical Data Network Radios

The advent of the information age has created organizational cultures that depend on data systems to communicate with each other to *push* and *pull* critical information. A U.S. military example of "*push and pull*" approach is the Global Broadcast System that defines "*push*" as disseminating information in high volumes to widely dispersed, low cost receive terminals, and users request, or "*pull*" specific pieces of information promoting an efficiency and higher data rates of communication (Military.com, n.d.). The U.S. Army and Marine Corps field artillery communities began pursuing the integration of automated systems in 1996 to streamline tactical control of fires, gain situational awareness, and a create common operating picture of friendly firing units on the battlefield. The resulting system is known as the Advanced Field Artillery Tactical Data System (AFATDS), which is designed to operate with the Army and Marine Corps tactical communication systems. The communication basis of the AFATDS was to share data through an internal local area network that exchanges information between different levels of fire command and control organizations. The transmitting and receiving of data is accomplished by using communications capabilities provided by the single channel ground and airborne radio system (SINCGARS), the enhanced position location reporting system (EPLRS), and the mobile subscriber equipment packet network (Boutelle, 1996, p. 16). Operating with these various systems has given the AFATDS a higher degree of flexibility in how it communicates and transfers data in tactical network centric environments.

Despite the success AFATDS has had in the recent conflicts in Afghanistan and Iraq by digitally processing thousands of accurate, successful, fire missions, the primary communication devices, EPLRS and SINCGARS, require line of sight to communicate, which limits its use in certain terrains and when operating between large distances. To mitigate these constraints, communication retransmission sites are emplaced throughout the battlespace to ensure *links* and *hops* between devices occur to obtain the information to its intended final destination.

The Marine Corps, as a means to prevent troop casualties due to "Friendly Fire," initiated the Position Location Reporting System (PLRS) during the later stages of the Vietnam conflict. Later, the U.S. Army initiated a program that would build on top of PLRS, but provide more communication capabilities. This program is now known as the Enhanced Position Location Reporting System (EPLRS). Today, the U.S. Army, Navy, and Marines use EPLRS as a position location, identification, and on some occasions, as a navigation system. The EPLRS consist of two primary components, an EPLRS network manager (ENM) and a network of radio sets (RS) (Tharp, 2003, p. 206). The network has several EPLRS RSs, which can be compared to network nodes and access points. ENM provides distributed management to the RSs that includes network planning, communication circuit information, system monitoring, fault detection and resolution, and security key management (Tharp, 2003, pp. 206–207). Currently, the Marine Corps uses EPLRS as a data radio deployed to serve as the data backbone among military echelons and provide data connectivity at battalion level, and on some occasions, at the company level. EPLRS primary mission in the Marine Corps is to act as a data link; however, it also provides position location of friendly units (Tharp, 2003, p. 209). These position reports are critical in maintaining a common operating picture (COP) and expediting fire support coordination in a fluid combat environment. Table 2 provides technical specifications and of the Marine Corps field data radio system EPLRS with images of both the RS and ENM laptop.

Enhanced Position Locating and Reporting System (EPLRS)	System Characteristics	Description	Locations
	***Tech:*** Digital ***Spectrum:*** UHF 420– 450 MHz frequency hopping ***Orientation:*** Omni-directional ***Mobility:*** OTM ***Power:*** Vehicular 4 Settings; 100, 20, 3, .4 watts. Man-pack RT; 16 watts ***Operational Mode:*** Data ***Distance:*** Terrain dependent, ground to ground per hop, max of 10 hops approximately 200 miles ground to air ***Encryption:*** Terminal Electronics Unit Transec Module	EPLRS currently consists of an ENM and radios that can be configured for man-pack or various ground platforms use. The AN/VSQ-2D(V)1 is a Data Net Radio that provides secure, jam-resistant radio frequency connectivity and positional location capabilities to the user. The main components of the Radio Set are a RT (RT-1720_(C)/G), an EDPA, a URO device for entering and receiving messages, and the appropriate installation kit for the platform from which it is to be operated. The ENM is a ruggedized laptop-based software program used to maintain the network.	***CE:*** MEU ***GCE:*** HQ Bn, Comm Co, Inf Regt, ELMACO, Inf Bn, Arty Regt., Arty Bn., AAV Bn, LAR Bn. Cmbt. Eng Bn ***ACE:*** MASS, MWSG, MWCS ***LCE:*** Comm Co

Table 2. USMC Tactical Data Radios (From: Marine Corps Systems Command, 2011).

C. AIRBORNE RELAYS

The limitations of line of sight radios motivate the military to explore methods to ensure persistent communications on the battlefield, such as the use of airborne relays. The concept of airborne relays gained attention during the Vietnam conflict. The U.S. military equipped helicopters with multiple FM radios to serve as airborne retransmission sites for voice nets and extended their C2 range. However, the helicopter radio relays only supported large-scale operations and were used for temporary amounts of time. The high cost of the aircraft operations prohibited the use of this technique for extended periods of time (Ryan, 2002, p. 293). Although helicopter airborne relays were not a long-term viable solution, due to high cost, other cost-effective alternatives have been explored over the years, such as airships, balloons, and unmanned aircraft equipped with communication payloads.

1. Airships

The concept of airships, also referred to as High Altitude Airships (HAA) or High Altitude Platforms (HAP), have been a focus of the U.S. military as a possible solution to meet the high demand for military communications. The U.S. military's commitments in Afghanistan and Iraq spiked the need for ground commanders to control forces over wide areas. To command and control these forces effectively, military commanders require reliable communication networks to support both voice and data transmissions over wide areas. SATCOM bridged some of the requirement gaps, but not enough satellite assets were available to support the expansive U.S. military communication requirements. The limited amount of satellites in orbit is attributed the high cost associated with this communication resource. The approximate cost of each geosynchronous satellite is $200 million dollars, which makes it cost prohibitive to assign dedicated SATCOM channels to each unit operating across two theaters, and other military commitments throughout the globe (Jamison, 2005, p. 5).

The DoD has commissioned several third-party consultant studies to find alternatives to augment the high priced satellite communications program. Certain third-party studies recommend the use of HAA as a viable alternative. HAAs are designed to maintain geostationary positions at approximately 65,000 feet (21.33 km), generate power through solar panels, and carry various communication payloads that can perform the functions of a satellite. These airships are not cheap and are estimated to cost approximately $50 million dollars per aircraft. However, in comparison to the cost of satellites, the airships could perhaps be a more cost-effective possibility for the U.S. military (Jamison, 2005, p. 3). Figure 3 is an artist's concept created for U.S. Missile Defense Agency (MDA) by Lockheed Martin, which was contracted to develop a prototype of HAA. HAA and HAP concepts have been proposed to the U.S. Army as possible surrogate satellite systems to augment and replenish space capabilities and bridge SATCOM shortages (Jamison, 2005, p. 3). The use of HAA vertical nodes can also reduce power requirements and latency times caused by the distance the signal must

travel to reach satellites from ground stations. The HAA are not the only vertical node platform options. Other cost effective means of enabling wide area communications include the use of tethered balloons equipped with communication payloads.

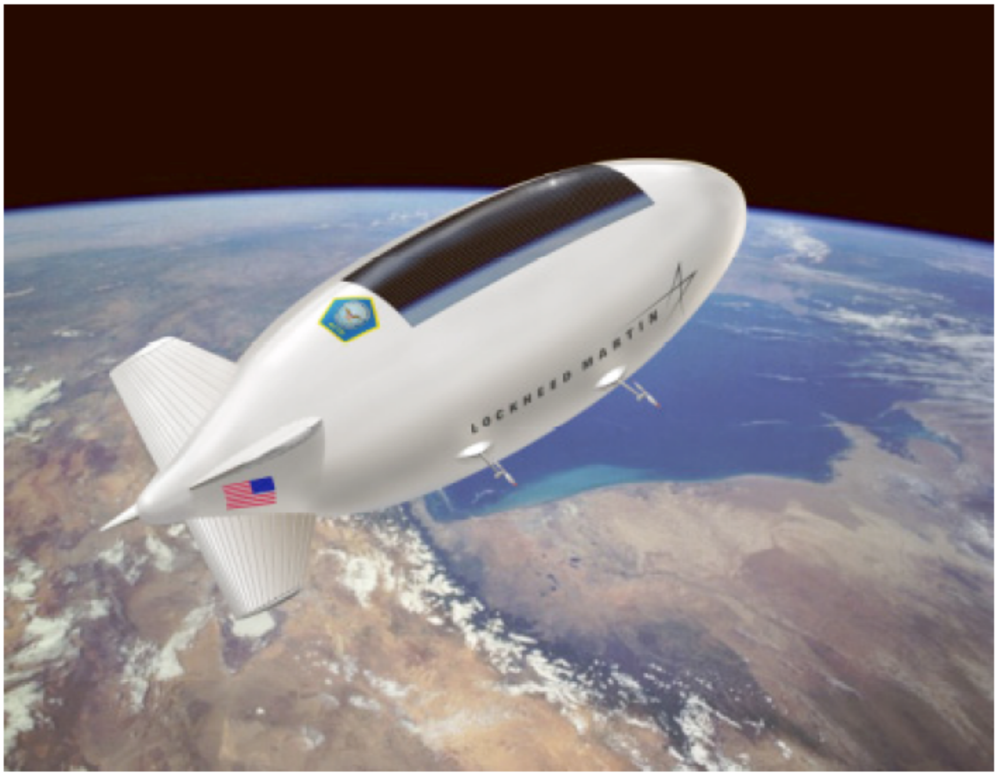


Figure 3. Artist's Concept of U.S. Missile Defense Agency Prototype by Lockheed Martin (From: Jamison, 2005, p. 10).

2. Balloons

The Marine Corps is employing the Combat SkySat helium balloon to reduce the need of SATCOM. The Combat SkySat system is used to retransmit both voice and data and extend the range of UHF communications. The system is comprised of a helium balloon with hanging antennas and radios that relay UHF signals using line of sight that mitigates the need for SATCOM. The Combat SkySat system flies between 55,000 and 85,000 feet, which is considered the Earth's stratosphere. At this altitude, the system is able to extend the Marines communication range up to a 600-mile radius. Figure 4 depicts a Marine with the 13th Marine Expeditionary Unit fielding the Combat SkySat

Balloon 2008. Since the initial fielding in 2008, the Combat SkySat system has proven to be successful in real world operations in Libya, Pakistan, and Afghanistan (Antoine, 2012, pp. 11–12). The primary use has been employing the balloons to command and control aircraft operating outside the communications envelope of amphibious aircraft carriers.

Figure 4. 13th Marine Expeditionary Unit fields Combat SkySat Communications Relay Balloon (From: Barker, 2008).

D. UNMANNED AIRCRAFT SYSTEMS

UAS have been the U.S. military's mainstay in the long war against terrorism, and are often referred to as UAV or UAS. The two terms do have significant differences as UAV refers only to the aircraft, whereas the term UAS is in reference to all parts that comprise the system, which includes ground stations, remote stations, communication link payloads, and visual sensors (Austin, 2010, p. 3). The uses of UAS have been traditionally associated with intelligence collection for the military or other government agencies in the Global War On Terrorism in recent years. However, the application of UAS has expanded to other functions that include prosecuting targets with the use of

weaponized platforms, communication relays, and logistical re-supplies to remote locations. In the communications field, UASs are being equipped with payloads that provide communication relay, hence making the UAS a relay node that forms networks that will enable communications and continuous feed flow from the ISR sensors. The DoD is pursuing dedicated net-centric UAS that can be emplaced in strategic locations to enhance military communication capabilities (Department of Defense, 2009, p. 15). Table 3 provides an all-inclusive list of UAS platforms associated with net-centric operations, according to the DoD's FY2009–2034 Unmanned Systems Integrated Roadmap. The list includes not only air platforms, but also ground and sea systems.

Named Unmanned Systems Associated with Net-Centric (NC)	
Broad Area Maritime Surveillance UAS (BAMS UAS)	Multi-function Utility/Logistics and Equipment (MULE) ARV Assault Light (ARV-A(L))
Class I UAS	Multi-function Utility/Logistics and Equipment (MULE) Countermine (MULE-C)
Class IV UAS	Multi-function Utility/Logistics and Equipment (MULE) Transport (MULE-T)
Communications Relay UAS	PackBot Explorer
High Altitude Persistent/Endurance UAS	PackBot FIDO
RQ-4 Global Hawk	PackBot Scout
STUAS/Tier II	Route Runner
Vertical Take-off and Landing Tactical Unmanned Air Vehicle (VTUAV Firescout)	Small Unmanned Ground Vehicle (SUGV)
MARCbot	xBot (PackBot Fastac)

Table 3. Unmanned Systems Associated with Net-Centric Architecture, FY2009–2034 Unmanned Systems Integrated Roadmap (From: Department of Defense, 2009, p. 15).

It has become a typical DoD practice to attempt to standardize or categorize units, equipment, and procedures as much as possible to avoid overlap and excessive redundancy. In the UAS arena, categorization also involves adhering to regulations set by other U.S. federal agencies. In the case of airborne systems, regulations set by the Federal Aviation Administration (FAA) were items of consideration and influenced the Joint categorization of the UAS platforms. Table 4 depicts the three categories set by the Joint UAS Center of Excellence and the FAA regulation to which they are aligned. The other criteria used to set categories include the airspace the UAS utilizes and the airspeed of the aircraft. The Joint Unmanned Aircraft System (JUAS) categorizations are beneficial for

services to understand the restrictions and parameters to which each platform must adhere at the highest levels of federal policy. However, the JUAS categorizations change at each individual service and further changes occur at different command levels within the services. Table 5 further defines the JUAS COE categorizations of UAS platforms.

		Certified Aircraft / UAS (Cat III)	Nonstandard Aircraft / UAS (Cat II)	RC Model Aircraft / UAS (Cat I)
FAA Regulation		14 CFR 91	14 CFR 91, 101, and 103	None (AC 91-57)
Airspace Usage		All	Class E, G, & non-joint-use Class D	Class G (<1200 ft AGL)
Airspeed Limit, KIAS		None	NTE 250 (proposed)	100 (proposed)
Example Types	Manned	Airliners	Light-Sport	None
	Unmanned	Predator, Global Hawk	Shadow	Dragon Eye, Raven

Table 4. Joint UAS Categories Aligned to FAA Regulations, FY2009–2034 Unmanned Systems Integrated Roadmap (From: Department of Defense, 2009, p. 95).

UAS Category I	Analogous to Remote Control (RC) models as covered in AC 91-57. Operators must provide evidence of airworthiness and operator qualification. Small UAS are generally limited to visual LOS operations. Examples: Raven, Dragon Eye
UAS Category II	Nonstandard aircraft that perform special purpose operations. Operators must provide evidence of airworthiness and operator qualification. Cat II UAS may perform routine operations within specific set of restrictions. Example: Shadow
UAS Category III	Capable of flying through all categories of airspace and conforms to Part 91 (i.e., all the things a regulated manned aircraft must do including the ability to survey and analysis.) Airworthiness certification and operator qualification are required. UAS are generally built for beyond LOS operations. Examples: Global Hawk, Predator.

Table 5. Joint UAS Center of Excellence UAS Category Definitions, FY2009–2034 Unmanned Systems Integrated Roadmap (From: Department of Defense, 2009, p. 96).

1. USMC Unmanned Aircraft Systems

The Marine Corps' overall 21st Century Expeditionary Maneuver Warfare (EMW) strategic vision closely integrates the employment and sustainability of UAS, whether its Ship-to-Objective Maneuver (STOM) or Distributed Operations, the Marines

intend to gain the advantage over their adversaries with the use of UAS. A central part of this strategy is to obtain secure timely intelligence with organic UAS assets. Therefore, the Marines have developed the Reconnaissance, Strike, and Target Acquisition (RSTA) capabilities program to ensure that procurement of UAS platforms meet specific USMC requirements. The RSTA capability requirements are focused on providing Marine commanders continuous awareness of the battlespace. This concept of awareness entails warnings of possible hostile forces or actions, and extracting detailed, precise, and sustained information on possible hostile forces and their actions (Isherwood, 2008, p. 14).

The use of UAS has enabled Marines at the lowest tactical levels to see beyond the next hill or beyond the next building in urban environments in both Afghanistan and Iraq. The Marine Corps has categorized UAS based on RSTA capabilities and the level of command the platform supports. Other factors taken into consideration when categorizing USMC UAS are maximum altitudes and ranges (see Figure 5). The groups or tiers are broken into three levels: tier 1 is flown at battalion and below, tier 2 is flown at division and below, and tier 3 flown at Marine Expeditionary Force and below. The tiers are operational control guidelines; however, if a battalion or below unit has a need for the use of a division level UAS asset, a tactical air request can facilitate the allocation. The Marine Corps has carefully selected platforms that meet the RSTA requirements and provide the Marine Air Ground Task Force commanders the organic UAS assets that will provide them with maximum situational awareness. Table 6 is a list of the current Marine Corps UAS inventory broken down by tier.

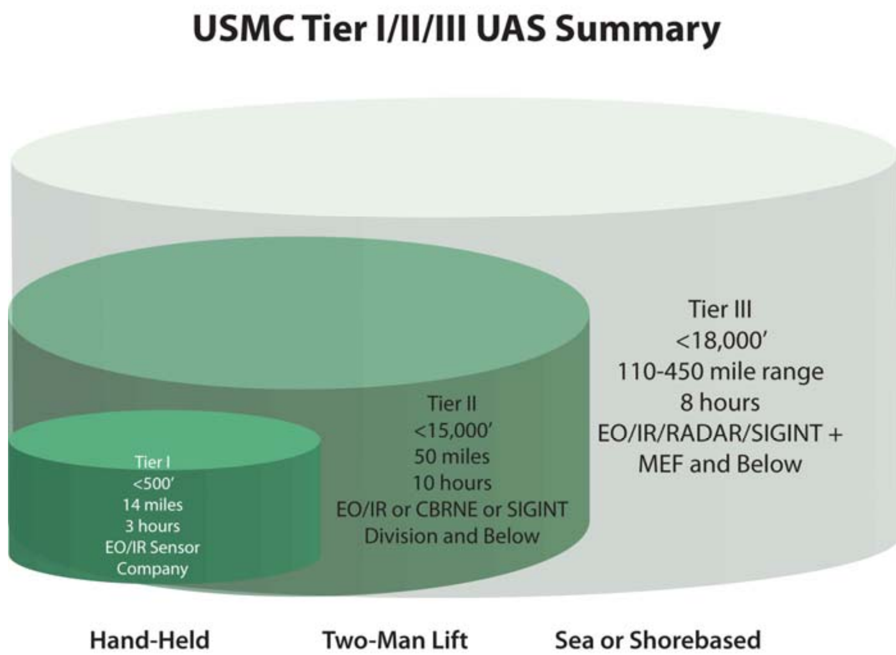


Figure 5. USMC UAS Categories and Command Tier Levels (From: Isherwood, 2008).

USMC UAS INVENTORY

WASP	**System Characteristics**	**Description**	**Performance**
	***Weight:*** 0.7lb ***Length:*** 11in ***Wingspan:*** 16in ***Payload Capacity:*** 25lb ***Engine Type:*** Electric Battery ***Tier:*** I	Rugged unmanned air platform designed for front-line reconnaissance and surveillance over land or sea. Wasp serves as a reconnaissance platform for the company level and below by virtue of its extremely small size and quiet propulsion system	***Ceiling (MSL):*** 10,000ft ***Radius:*** 2-3 nm ***Endurance:*** 60 min ***Cruise Speed:*** 15-35kt ***Sensor:*** 2 color cameras
RQ-14 Dragon Eye	**System Characteristics**	**Description**	**Performance**
	***Weight:*** 4.5lb ***Length:*** 2.4ft ***Wingspan:*** 3.8ft ***Payload Capacity:*** 1lb ***Engine Type:*** Battery ***Tier:*** I	Company/platoon/squad level with an organic reconnaissance, surveillance, and target acquisition (RSTA) capability out to 2.5 nautical miles	***Ceiling (MSL):*** 10,000ft ***Radius:*** 2.5nm ***Endurance:*** 45-60 min

Raven 11B	System Characteristics	Description	Performance
	***Weight:*** 4.2lb ***Length:*** 36 in ***Wingspan:*** 55 in ***Payload Capacity:*** 11.2oz ***Engine Type:*** Direct Drive Electric ***Tier:*** I	Remotely controlled from its ground station or fly completely autonomous missions using global positioning system (GPS). Standard mission payloads include EO color video with electronic stabilization and digital Pan-Tilt-Zoom or an IR camera.	***Ceiling (MSL):*** 15,000ft ***Operating Altitude (AGL):*** 500ft ***Radius:*** 10km (LOS) ***Endurance:*** 90 min ***Cruise Speed:*** 26 knots
RQ-7 Shadow 200	**System Characteristics**	**Description**	**Performance**
	***Weight:*** 375lb ***Length:*** 11.33ft ***Wingspan:*** 14ft ***Payload Capacity:*** 60lb ***Engine Type:*** MOGAS ***Tier:*** II	Shadow is rail-launched via catapult system. Its gimbaled upgraded plug-in optical payload (POP) 300 EO/IR sensor relays video in real time via a C-band LOS data link and has the capability for IR illumination (laser pointing)	***Ceiling (MSL):*** +14,000ft ***Radius:*** 125km ***Endurance:*** 5-6 hours ***Cruise Speed:*** 110 knots
ScanEagle	**System Characteristics**	**Description**	**Performance**
	***Weight:*** 37.9lb ***Length:*** 3.9ft ***Wingspan:*** 10.2ft ***Payload Capacity:*** 13.2lb ***Engine Type:*** Gasoline ***Tier:*** II	ScanEagle carries an inertially stabilized camera turret for EO/IR imagery. Its sensor data links have integrated cursor-on-target capability, which allows it to integrate operations with larger UAS such as Predator through the GCS.	***Ceiling (MSL):*** 16,400ft ***Radius:*** 60nm ***Endurance:*** 15 hours ***Cruise Speed:*** 70/49 knots

Table 6. USMC UAS Programs of Record, FY2009–2034 Unmanned Systems Integrated Roadmap (From: Department of Defense, 2009, pp. 69–76).

The author executed operational control of AeroVironment Raven 11B at the Brigade Platoon level for 1st Air Naval Gunfire Liaison Company (ANGLICO) during an Afghanistan deployment in support of Operation Enduring Freedom 2010. Although the Marine Corps categorizes the Raven 11B as battalion level asset, many occasions arose during the deployment when the Raven 11B was deployed to support four-man teams and small convoy operations. During convoy operations on hostile unimproved roads, the Raven 11B was hand launched from tactical vehicles and piloted on the move. The Raven 11B was a critical asset for route reconnaissance and observation posts to detect hostile activity while on the move. The author's assessment of the Raven 11B is that it is a

versatile and a scalable intelligence, reconnaissance, surveillance platform with a high potential to perform multi-missions, such as communication relay for battalion, company, platoon, and team-level operations in austere environments.

E. COMMERCIAL OF THE SHELF TECHNOLOGY

The advances in telecommunications in recent years, such as the introduction of smart phones and tablets, have inspired the military to leverage similar designs. Military tactical radio designers are adding more innovative features and functions that parallel those used in commercial smart mobile devices. This trend is leading the new generation of tactical radios that provides service members with devices that are more flexible, simpler to operate, and lighter in weight (Edwards, 2012, p. 1). Although tactical radios, such as the Harris AN/PRC-117G, are not necessarily COTS product, Harris has emulated COTS technology to provide the military with comparable solutions. The AN/PRC-117G tactical radios have been designed to support network centric operations to allow soldiers and Marines to build mobile ad-hoc networks (MANET) using the AN/PRC-117G and access features, such as e-mail and chat on the battlefield by attaching small personal devices, such as notebook computers and tablets, to a secure radio tactical network. These end-devices offer soldiers and Marines user interfaces similar to those of COTS smartphones.

The need for tactical radios will continue to exist; however, high interest exists in having military specific radios and COTS technology integrate and maintain the level of security required by the DoD. The integration of military specific design and COTS can also add to cost savings by eliminating the military's need for research and development. The military is also exploring options on to how introduce COTS mobile devices into the tactical environment as it realizes that a smartphone averages approximately $200 dollars, instead of the $17,000 for military-specific, tactical radios (Edwards, 2012, p. 1).

F. SUMMARY

This chapter attempted to provide a general appreciation and context of the overall state of U.S. military communication systems, procedures, and the road ahead. Significant advances have been made in communication technology and the goal is for

these advances to be shared across the entire military spectrum, and promote that they can reach the lowest common denominator on the frontlines. The following chapter narrows the scope and provides technical background information on the equipment intended for use in the field demonstration and tests the proof of concept of the Small-UAS airborne vertical network node.

THIS PAGE INTENTIONALLY LEFT BLANK

III. TECHNOLOGICAL BACKGROUND

A. INTRODUCTION

In the literature review, the origins of tactical communications and the various equipment associated with ensuring commanders the ability to command and control troops in wide areas were presented. Additionally, discussed and described were the latest communication technologies being employed by the military, with an emphasis on the United States Marine Corps. The literature review also placed a particular focus on the operational employment of UASs, again with an emphasis on Marine Corps systems. These two particular areas are growing exponentially within the U.S. military and advancements in communication technology are allowing for compact end devices, smaller signatures, and increased capabilities. At the strategic level, UASs are our being designed for multi-missions to enhance the military's enterprise communication infrastructure. Multi-mission UASs, such as the U.S. Army's I-GNAT "Warrior Alpha," will have the ability to provide commanders with more than just ISR and weapons employment capabilities, but also offer global communication links. Strategic level UASs with robust communication payloads will have the ability to perform missions that can be equated to surrogate satellites (Department of Defense, 2009, p. 61).

This research is to pursue similar capabilities; however, the objectives are to bring the airborne vertical relay node concept to the lowest common denominator, "The Warfighter." Within government and DoD civilian leadership, the term "warfighter" encompasses a very large spectrum, it begins with the rank of four-star general and ends at the rank of private. In the Marine Corps, a three-star general commands a Marine Expeditionary Force (MEF), and this position is considered to be at the warfighter level. The same can be said of the four-star generals commanding the various regional combatant commands. Hence, "warfighter" is a term that applies to several layers of the military; in this case, in particular, it connotes a strategic-level role.

The strategic level warfighter has great responsibility; he is usually in charge of several thousand troops and large geographical areas. To perform the mission

successfully he requires a robust support infrastructure that includes satellites, ground control stations, fiber optic landlines, and so forth. In the case of a Marine Air Ground Task Force, such as a MEF, the commanding general is responsible for approximately 43,000 Marines and sailors. Similar to a strategic-level general, the operations-level general requires robust communications infrastructure to perform his duties. Figure 6 depicts the MEF's doctrinal, organizational chart, extracted from USMC doctrinal publication MCRP 5-12D. The organizational chart demonstrates the various layers within a combat organization and how a finite amount of resources must be distributed throughout the various levels of the war-fighting organization. In the chart, the Command Element (CE) is where the three star commanding general resides and the lowest common denominator, the private, resides inside a battalion, within a regiment. The intent for the airborne vertical network node concept is to bring comparable levels of communication services across all levels, with an emphasis on company and below units. To achieve this goal, the integration of tactical radio networks and UAS systems is being suggested to provide users with adequate, persistent, reliable, tactical communication services.

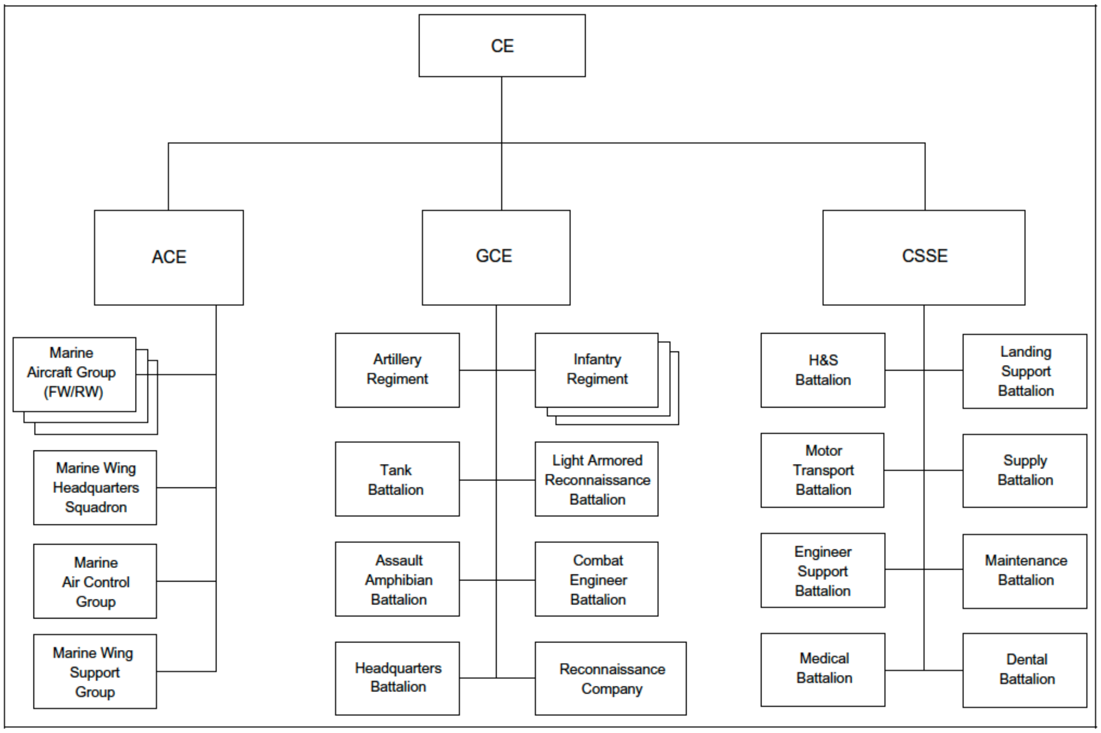


Figure 6. Marine Expeditionary Force Task Organization, MCRP-5-12D (From: United States Marine Corps, 1998, pp. 2–3).

B. PREVIOUS EFFORTS

The concept of airborne relay vertical communication relay nodes is not new. During the Vietnam conflict, U.S. military forces equipped helicopters with multiple radios to provide interim tactical communications networks. These airborne voice command nets provided commanders the ability to command and control troops during the commencement of major offensive operations. Leveraging the tactical agility and tasking responsiveness of air assets, the airborne relays provided ground communication units time to establish hardened retransmission (“relay”) sites for follow-on operations (Ryan, 2002, p. 293). However, as a long-term solution to the military’s LOS radio frequency (RF) constraints, this tactic was not a viable option, as the cost of flying a manned aircraft exclusively to perform communication relay is cost prohibitive. The limiting factors are the high cost associated with aircraft maintenance, fuel, and manpower, as well as the airframe itself. However, the introduction of UAS technology

has reopened the exploration of airborne vertical nodes. The cost of operating and maintaining UASs is significantly lower than manned aircrafts, which makes the concept more affordable and appealing during periods of budgetary constraints.

In this research, two similar studies were reviewed that attempted to leverage UAVs as vertical communication relay nodes. The first study was a collaborative project between the Marine Corps Warfighting Laboratory and the Naval Research Laboratory. The focus of this study was the integration of a VRC-99A network radio and a Kaman K-MAX helicopter to enable over-the-horizon communications for Marine Expeditionary Units (MEUs) and Amphibious Ready Groups (ARGs.) These two organizations are comparable in size to a reinforced land army regiment, which are a few layers above the scope addressed in the proof of concept. The second study encountered was a thesis project by a Naval Postgraduate School (NPS) student, LT John P. Richerson, United States Navy (USN). LT Richerson's research was centered on the integration of Wi-Fi 802.11 technology and rotary UAVs. His work placed great emphasis on COTS technology for both mini-rotor UAV options and Wi-Fi access point devices. A description of each of these follows.

1. Dragon Warrior Communication Relay Testing

The Marine Corps Warfighting Lab, in partnership with the Naval Research Laboratory, conducted a test in 2002 of the use of a Kaman K-MAX UAV with a communication payload to provide a near-term solution for unmanned aerial communications relay. This concept would equip MEUs ARGs with over-the-horizon links for networked data communication. The Dragon Warrior communication suite would implement a wideband TCP/IP data network for dispersed Marine units ashore and a reach-back capability with ARG ships over-the-horizon (Tate, 2003, p. 1).

a. Airborne Relay Configuration

The airborne relay communications payload consisted of an AN/VRC-99A network radio and a Panasonic Toughbook laptop that served as the Communication Relay Controller (CRC). The BAE Systems AN/VRC-99 radio is a ground vehicle, airborne, and shipboard configurable radio, with the following capabilities, end-to-end

connectivity, packet formatting, and packet switching protocols (Jane's Information Group, 2009). The radio and laptop have specific power requirements; therefore, a DC-DC converter was added to the payload that added weight and bulk. The VRC-99A and the laptop were connected via a 10Base2 Thin Ethernet. Lastly, a connection between the payload and the aircraft avionics, via RS-232 serial interface, gave access to the remote management system, in which the GPS device is housed. The VRC-99A radio used for the test was a direct-sequence spread-spectrum network radio that could support data rate bursts of 625 Kbps to 10 Mbps in networks of up to 16 radios, and operated in the frequency range of 1308 to 1484 Mhz (Tate, 2003, p. 3). Figure 7 is an image included in the report that illustrates the components used in the test; but more importantly, it depicts the sizable payload that had to be integrated into the UAV.

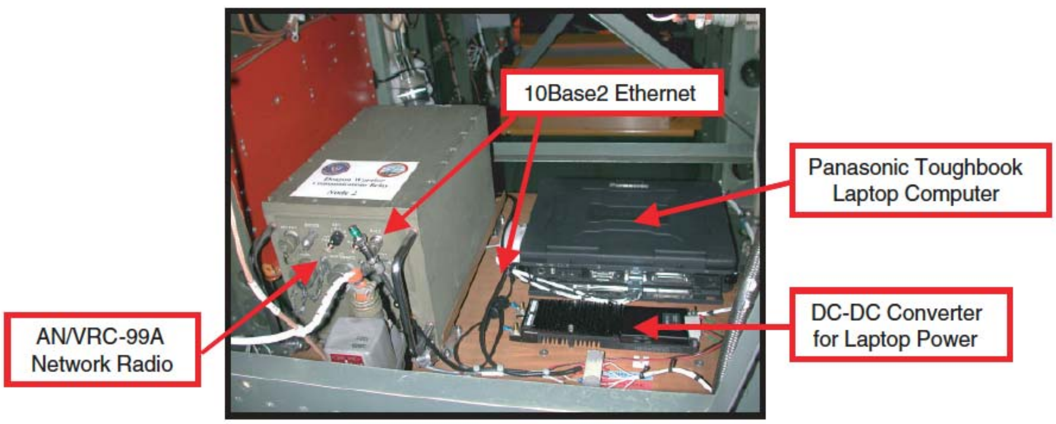


Figure 7. Dragon Warrior Test Communication Relay Payload (From: Tate, 2003, p. 4).

The Kaman K-MAX manned or unmanned helicopter was selected for the Dragon Warrior test. The Kaman KMAX is a multi-mission helicopter that can be flown by a pilot in the aircraft or flown remotely from a ground station. The K-MAX capabilities include a 12-hour endurance flight time, BLOS control, programmable waypoint navigation, auto-land/auto-take off, range of 185km, and a payload capacity of

6,000 lbs (Kaman, n.d.). Beyond the Dragon Warrior test, the K-MAX UAV was not integrated as a communications relay platform, although the Marine Corps did procure the aircraft for unmanned aerial resupply missions.

The results of the test drew several conclusions on the equipment used and the environmental impacts in attempting to achieve test goals. The Dragon Warrior test team concluded that the VRC-99A requires clear LOS to operate even in relatively short distances. The VRC-99A operates in the L-band frequencies. It was observed that foliage and buildings affect the signal. The test team was able to achieve their goal of conducting a 50nm communication relay over water successfully. To achieve the communication shot at that distance, the team observed that the UAV had to be at an altitude of 6000 ft or higher. The Dragon Warrior test has encouraged other researchers to investigate how to integrate communications equipment and UAV platforms successfully to increase their functionalities.

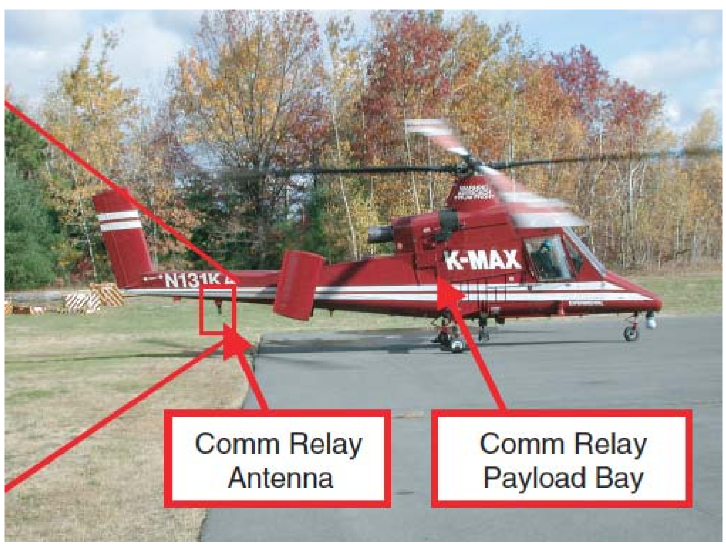


Figure 8. Dragon Warrior Test UAV, KAMAN K-MAX (From: Tate, 2003, p. 5).

2. Extension of Wireless Mesh Networks via RC VTOL UAV

The objective of the 2007 NPS thesis by LT Richerson, USN, was to integrate a Wi-Fi 802.11 wireless LAN access point with a mini vertical takeoff and landing rotary UAV to extend a client based network. In addition to successful integration of Wi-Fi and

UAV, LT Richarson's field experiments were designed to test and evaluate the durability of COTS components and how they would withstand demanding tactical environments. Much like the primary objective of this thesis, LT Richerson's integration of Wi-Fi 802.11 and mini-rotor UAV was an attempt to enhance the communication capabilities of the tactical user via vertical nodes.

a. Wi-Fi Extension Via VTOL UAV Configuration

The Wi-Fi 802.11 wireless test payload consisted of a Mesh Dynamics 4000 circuit board, an external battery to power Wi-Fi device, and the Mikado Logo 24 vertical takeoff and landing (VTOL) mini rotary wing airframe (Richerson, 2007, p. 35). The Mesh Dynamics 4000 operated at 2.4 GHz and measures of performance were based on transmissions using Internet Protocol, Transmission Control Protocol, and User Datagram Protocol. The Mikado Logo 24 UAV is a COTS platform and categorized as a RC aircraft. The author did not include specific testing altitudes.

The test report indicate the Mesh Dynamics 4000 wireless access point provided a 10 Mb/Sec networking solution. Other observations included that the UAV surrogate could provide a control link for associated autonomous flight packages with the use of the TCP/IP protocol pair (Richerson, 2007, p. 63). The experiment also encountered frequency conflicts between the RC helicopter and the embedded communication device, which underscored the importance of frequency management of both the UAV control system and the communications payload.

Figure 9. Mikado Logo 24 RC Helicopter equipped with Mesh Dynamics 4000 Wi-Fi Wireless Access Point (From: Richerson, 2007, p. 35).

C. SMALL-UAS TEST TECHNOLOGICAL BACKGROUND

The overall technological goal is to provide innovative methods to solve existing problems with non-developmental equipment to avoid the high costs of research and development, production, and procurement. In the initial test construct, the use of existing military communication hardware was planned to avoid the cost and time associated with a formal acquisition process. The premise of the concept was also founded on the ability to reuse existing inventory in times of budgetary constraints. While not opposed to using a COTS communication system, not all COTS devices however meet the National Security Agency Type 1 security standards and have limited military application. At the time of the testing, suitable Type 1 security devices small enough to embed into the Raven 11B were not available and a COTS option for testing was used instead. For the proposes of this thesis, the COTS devices selected for the test are similar to what the U.S. military has adopted in recent years, including tactical radios with waveform technology that form ad hoc wireless networks, which extends range and mobility, and commonly known as wireless mesh networks in the commercial telecommunication industry.

1. Wireless Mesh Networks

Wireless mesh networking has become a popular method for telecommunication companies to extend their fixed networks and offer greater mobility to users. The concept

of mesh networking can be best described as a collection of *n* nodes, or communicating devices, that exchange data among one another. Each node has the ability to communicate with other nodes on the network and transport, route, and share data with neighboring devices. The process of nodes communicating with other nodes represents a mesh network topology (Held, 2005, p. 3). In a wireless environment, mesh networking may be achieved by using common single RF transmitter/receiver for the nodes, which have the ability to communicate with virtually every other node as long as they are within range of each other. If a particular node receives data but that data is intended for a different recipient, then the receiving node will retransmit the data (relay) as necessary and as determined by the network's routing process.

Wireless Local Area Networks (WLANs) fall into two categories. The first is known as an ad hoc networking in which each node communicates directly with the other reachable wireless nodes, and the second is known as an infrastructure WLAN, in which all traffic is routed through an access point (AP) (Held, 2005, p. 5). When using the infrastructure WLAN, a potential exists that communications may suffer if the AP becomes non-operational. To address these types of problems, nodes in ad hoc networks can be configured to function as relays, or repeaters, which eliminates the dependence on an AP. Figure 10 is a graphic depiction of a wireless mesh network in an ad hoc environment in which each node functions as a router and repeater. For the testing and demonstration phase, Persistent Systems Wave Relay® radio systems were selected based on Mobile Ad Hoc Networking.

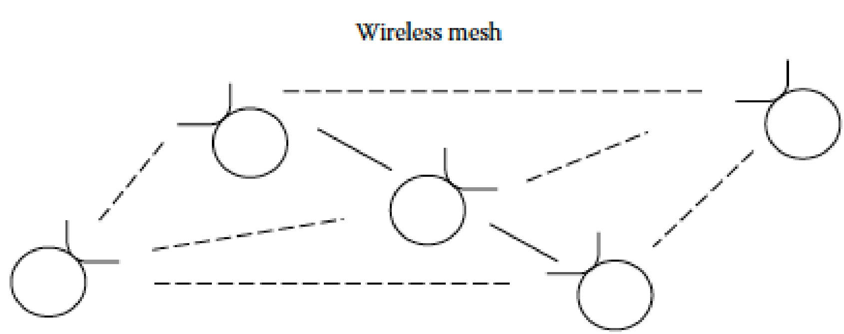


Figure 10. Wireless Mesh Network Consisting of Five Nodes, Introduction to Wireless Mesh Networks (From: Held, 2005, p. 6).

2. Mobile Ad Hoc Networks

Mobile Ad Hoc Networks or MANET's are an autonomous collection of mobile devices that form a self-configuring network that communicate using multi-hops within nodes. The mobility of the nodes distinguishes the MANET from other ad hoc networks in which the nodes are not mobile. MANETs are decentralized and do not require existing infrastructure All network activity, including discovering the topology and delivering messages, must be executed by the nodes themselves. To execute these tasks, the mobile nodes must have routing functionality incorporated into the mobile devices (National Institute of Standards and Technology, n.d.). For the test and demonstration of this thesis, the Persistent Systems Wave Relay™ radio systems that uses MANET wireless configurations in its mobile devices was selected. Although Wave Relay™ cannot be widely used in military applications because it does not meet National Security Agency Type 1 encryption standards, for this thesis, it provided the demonstration with the required capabilities to validate that adding a wireless radio device to the small-UAS made it possible to form an ad-hoc network able to communicate BLOS and on-the-move in a austere field environment.

3. Communication Mobile Devices

Equipment that would simulate mobile devices currently in use in the U.S. military was required for this testing and demonstration of the small-UAS airborne vertical communication node. The closest systems readily available were the Persistent Systems Wave Relay™ radios that offered the ability to conduct voice, and data transmissions. The demonstration model required the equipment to operate within a maximum of 4-kilometer radius, which Wave Relay™ met and exceeded. The devices support push-to-talk voice transmission, as well as support popular TCP/IP protocols that made it possible to capture data for follow on test comparison analysis.

a. Wave Relay Quad Radio Router

The Wave Relay™ Quad Radio Routers are MANET wireless devices packaged in compact ruggedized cases. Each unit contains four separate wireless radios with the ability to perform package routing functions. Each Quad Radio operated may be

procured in one of several frequencies, to include but not limited, to 700 MHz, 900 MHz, 2.3-2.4 GHz, and 5.8 GHz. The router has a proprietary algorithm that selects the strongest signal path to communicate with neighboring nodes. The Quad radio can be mounted on a vehicle to offer mobility and flexibility in dynamic remote environments. The Quad radio can also be mounted on a mast for fixed sites and long-term static operations (Persistent Systems, n.d.). Figure 11 is a detailed diagram of the Quad Radio ports, interfaces, and antenna connections. It also provides a schematic displaying how auxiliary peripherals connect to the unit. Table 7 provides further technical specifications and capabilities of the Wave Relay™ Quad Radio Router. For this demonstration, the Wave Relay® Quad Radio Router was used as the ground nodes.

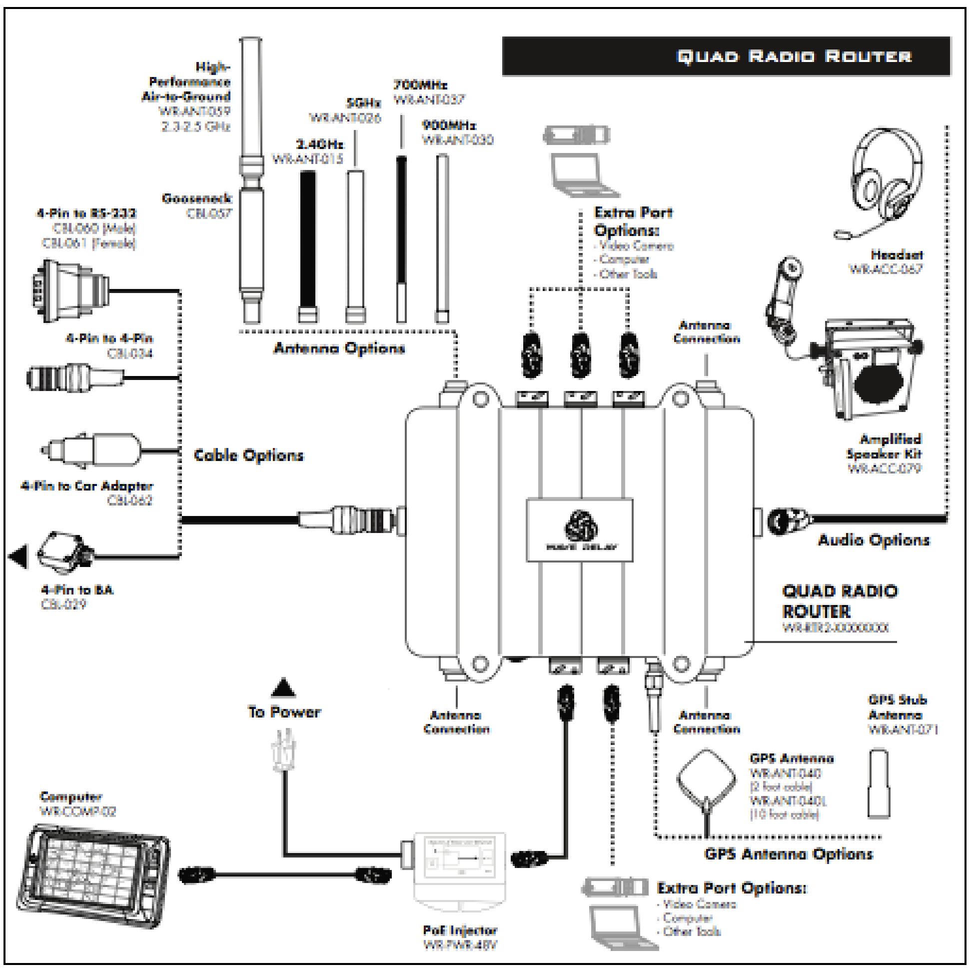


Figure 11. Wave Relay® Quad Radio Specification Diagram, Persistent Systems (From: Persistent Systems, n.d.).

Networking	Voice	Security	Radio	Mechanical	Power
- MANET routing -Layer 2 Connectivity -IPV4 -Integrated DHCP client/server -802.11a/b/g AP concurrent with MANET	-16 Channels of Push-to-Talk voice -Single or Multi-Channel mode -G.711 codec for Radio-over IP (RoIP)	-FIPS 140-2 Level validated by NIST -AES-CTR-256 with SHA 512 HMAC -AP Encryption-WPA-PSK	- OFDM with Adaptive Modulation Algorithms -Channel Width 5,10,20, and 40 MHz -Support for various RF bands	Size 8.5x6x2 inches -Weight 3.2lbs -Radio (4) RP-TNC antenna connectors -Integrated GPS receiver -PoE (1) port	Input voltage 8-48 VDC via PoE -Power consumption less than 16w

Table 7. Wave Relay™ Quad Radio Router Technical Specifications, Persistent Systems (From: Persistent Systems, n.d.).

b. *Wave Realy Single Board Module Payload*

At the time of the demonstration, a specific designed payload for the Small-UAS was not available. However, research associates, in collaboration with Persistent Systems, were able to acquire Wave Relay™ components configured on a scalable single board radio module. The Wave Relay™ single board radio module resembles an internal network card and has no protective case. These modules are available directly from Persistent Systems or through third party vendors, some of which offer them on the NASA SEWP program. The minimalist design of the module makes it lightweight and versatile, which made it possible to mount it onto the Small-UAS and test the airborne vertical network node proof-of-concept. Figure 12 is an image of the single board radio module prior to being mounted onto the Small-UAS.

Figure 12. Wave Relay™ Single Board Radio Module Small-UAS Payload

c. Power Source

The Wave Relay™ single board radio module does not have an organic power supply; hence, it was necessary to find a suitable lightweight battery pack to mount onto the side of the fuselage of the Small-UAS. A compact radio control modeler rechargeable battery with the capacity to power the radio for extended periods of time and not cause too much disturbance to the Small-UAS's airworthiness was selected. The Thunder Power 2250mAh 3-Cell/3S-11.1V rechargeable battery weighs 189 grams, and measures 26x35x102 millimeters (Thunder Power RC, n.d.). Figure 13 depicts the battery pack used to power the single board radio during the testing and demonstrations.

Figure 13. Thunder Power 2250mAh 3-Cell Rechargeable Battery Pack

D. UAS TEST PLATFORM

During the author's deployment to Afghanistan in support Operation Enduring Freedom 2009–2010, he had Raven 11B as part of his organic capabilities set. At the time, he was assigned to 1st Air Naval Gunfire Liaison Company and employed the Small-UAS as an extension of the Joint Terminal Attack Controller and Forward Observer fires suite. The Small-UAS was used routinely during convoys and in conjunction with observation posts to locate and target enemy forces. The platform is lightweight and man portable; its hand launch capability eliminates the need for special additional equipment. These attributes weighed heavily on the selection of the Raven 11B as the Small-UAS airborne relay test platform.

Additionally, the AeroVironment Raven 11B is a program of record both in the U.S. Army and U.S. Marines. Being a program of record means that it has been vetted through the DoD acquisition process and is officially part of the inventory, which is particularly important to the reuse philosophy and the prevention of further procurement of platforms that may have overlapping capabilities. The goal is to be able modify existing equipment, like the Raven 11B, to perform multi-missions and generate a greater return on investment. Another benefit to using an existing platform the elimination of the cost associated with training operators to fly a new UAS platform. The Raven 11B has been in the inventory for more than three years and each U.S. military service has a robust amount of experienced operators in their ranks.

1. Aerovironment Raven RQ 11B

The Raven RQ 11B is used primarily as a low-altitude intelligence, surveillance, and reconnaissance platform. The Raven RQ 11B can be operated manually or programmed to conduct autonomous flight by programming waypoints into its GPS navigation system (AeroViroment Inc., n.d.). Table 8 provides technical specifications on the Raven RQ 11B's range, endurance, and other system properties. Figure 14 shows images of the Raven RQ 11B system, which includes both an aircraft and a ground control station.

Figure 14. AeroVironment Raven 11B UAS System (From: AeroViroment Inc., n.d.).

Description	Specification
Payload	Dual Forward and Side-Look EO camera nose, Electronic Pan-tilt-zoom with stabilization, Forward and Side-Look IR camera nose (6.5 oz.)
Range	10Km
Endurance	60-90 minutes (rechargeable battery)
Speed	32-81Km/hr. 17-44knots
Operating Altitude	100-500ft AGL, 14,000ft MSL Max Launch Alt
Wing Span	4.5ft
Length	3ft
Weight	4.2lbs
Launch and Recovery	Hand-Launched, Deep Stall Landing

Table 8. AeroVironment Raven RQ 11B Technical Specifications (From: AeroViroment Inc., n.d.).

E. PERFORMANCE MEASUREMENT TOOLS

As Information Technology professionals, it is customary to find cost effective and efficient solutions to network inadequacies. To make logical decisions when investing in technology, it is essential to analyze the impacts on both the organization and the end-user. To assist in the process, it is preferable to have some form of relative values to measure the importance and the value added to the system. In the proof-of-concept, both roles are assumed, end-user and network designer. As an end-user, the viewpoint

occurs through a qualitative glass and the desire for things to work and not ask how they work. As network designers, situations are viewed from a quantitative perspective and require numerical values to compare performance gains or losses.

To capture relative values during the airborne vertical relay testing, an open-source network performance tool named Iperf was used. This tool provides network statistics about bandwidth, datagram loss, and latency. Iperf has an option to test the performance of Transfer Control Protocol (TCP) or User Datagram Protocol (UDP), the two commonly used transport layer protocols for Internet systems. The use of Iperf will provide statistical samples to make a comprehensive assessment of how the introduction of an airborne vertical node affects the performance of a tactical network.

2. Network Performance Measuring Tool

The National Laboratory for Applied Network Research (NLANR) and the Distributed Applications Support Team (DAST), based at the University of Illinois, developed the Iperf software. Iperf measures the maximum TCP and UDP bandwidth performance of a network. As mentioned earlier, Iperf reports bandwidth, delay jitter (UDP), and datagram loss (UDP) (SourceForge, n.d.). TCP and UDP are network communication industry standards, particularly the Internet Engineering Task Force (IETF) standards (RFCs) for transport layer protocols for use on the Internet. They were used in this demonstration to capture performance benchmarks.

a. Transmission Control Protocol

TCP has been the mainstay protocol for the Internet communication for over 30 years. TCP is known as a connection-oriented, end-to-end reliable transport protocol designed to fit in layered hierarchy and support multi-network applications. It was developed to operate above a wide spectrum of communication systems from hard-wired connections, packet-switched, and now, wireless networks (Information Sciences Institute, University of Southern Califronia, n.d.b.).

b. User Datagram Protocol

UDP is a connectionless protocol that functions in a broadcast-like manner, in which the acknowledgement of packet receipt is not required. It is popular for real-time and loss-tolerant applications, such as video feeds and audio (Voice over IP). UDP provides a procedure for application programs to send messages to other application programs with minimum protocol mechanisms. The drawback is that the protocol is transaction-oriented and delivery is not guaranteed (Information Sciences Institute, University of Southern Califronia, n.d.a.).

E. SUMMARY

This chapter examined previous work conducted in the field of tactical airborne vertical network nodes and discussed their findings. An attempt was made to apply their lessons learned and their future recommendations to gain further interest in the topic and influence a wider interest in airborne vertical nodes to bridge inadequacies in the field of tactical communications. Also provided was a technical background of the hardware and software used in the test and field demonstration. The following chapter explains the demonstration methodology, baseline tests, and field data analysis.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. SMALL-UAS AIRBORNE RELAY TEST METHODOLOGY AND RESULTS

A. INTRODUCTION

As a means to evaluate the airborne network relay node proof-of-concept and produce recommendations with qualitative and quantitative values, a series of demonstrations and tests were established. The main objectives for these tests were to prove the functionality of the airborne vertical relay node in communication areas identified to be deficient. The first goal was to demonstrate how the use of the airborne relay could enhance beyond light of sight communications at company-and-below military units. The second goal was to demonstrate how the airborne node could augment on-the-move communications and extend the range of tactical radio networks.

However, the objectives are not strictly technical in nature while always conscious of the difficulties involved in implementing exuberant costly ideas, especially if they must be vetted through the DoD acquisition program. Instead of pursuing the initiation of a new program, the goal is to leverage existing equipment in the U.S. military inventory that can be marginally modified to perform multi-missions.

In planning and executing the demonstrations and tests, the researchers were adamant about using equipment classified as programs-of-record, as it is officially in operational use within the U.S. military, and follow-on procurement actions are much simplified. However, due to unavailability, the radios used during the demonstrations and tests were not from a mainstream program-of-record. At the time of these tests, Harris Communications Corporation, the defense contractor that supplies a significant portion of U.S. military tactical radios, did not have a radio transmitter that could be utilized with the Small-UAS. Nonetheless, the tactical radio systems selected for the tests have generated interest among within the U.S. military and are being fielded by the special operations community. The Small-UAS platform used was the Raven RQ 11B, an existing program of record that has been in service for over three years.

The demonstrations and tests were carefully planned to simulate field environments, and on all occasions, active duty military personnel were involved. In addition to military personnel, military vehicles and equipment were also used to replicate the environmental conditions in which the airborne relay would be employed.

B. TESTING METHODOLOGY

The author's previous operational experiences in Iraq and Afghanistan with small level units included support to U.S. Marine and U.S. Army military transition teams, and allied special operation units as a fire supporter and joint terminal attack controller. Based on these experiences, the areas of focus and the test parameters to replicate tactical scenarios were narrowed. The test parameters included defined distances, static two-way voice transmissions, on-the-move two-way communications, and data transmission in communication-degraded environments. The premise of the tests and demonstrations was to gather performance data from stationary ground-based line-of-sight tests and establish a performance baseline. Once the baseline data were collected, performance data was gathered for the airborne relay node in field environments. Both data sets were used to create comparison models using statistical techniques, for example, normal distributions, null hypothesis, test statistic, and probability values. For the associated voice transmission tests, a qualitative approach was used by establishing a subjective scale that best represented the clarity of the transmission.

1. Test Construct

When constructing the test models, the goal was to be able to assess a quantitative value associated with the integration of Small-UAS airborne relay nodes in tactical environments. It was concluded that the best approach to assess that value was to compare the concept with existing communications practices. As mentioned in previous chapters, the majority of tactical communications are dependent on LOS and most communication links are achieved via ground stations, especially in tactical environments. Therefore a test was created that would capture data between two static ground stations to provide a baseline of throughput averages. The same process was

followed when introducing the airborne vertical relay node into the tactical radio network. Table 9 depicts both the dependent and independent variables and the comparison model for the data throughput transfer rates portion of the tests.

Distances	Baseline TCP Mbits/Sec	Air Relay TCP Mbits/Sec	Baseline UDP Mbits/Sec	Air Relay UDP Mbits/Sec
1 kilometer	Avg. Transfer Rates	Avg. Transfer Rates	Avg. Transfer Rates	Avg. Transfer Rates
2 kilometer	Avg. Transfer Rates	Avg. Transfer Rates	Avg. Transfer Rates	Avg. Transfer Rates
3 kilometer	Avg. Transfer Rates	Avg. Transfer Rates	Avg. Transfer Rates	Avg. Transfer Rates
4 kilometer	Avg. Transfer Rates	Avg. Transfer Rates	Avg. Transfer Rates	Avg. Transfer Rates

Table 9. Airborne Relay Node TCP & UDP Effectiveness Comparison Model

For the voice transmission baseline, a qualitative approach was used to measure effectiveness. Signal strength values based on the clarity of two-way Radio-over-IP (RoIP) transmissions were subjectively assigned. Similar to the data transfer comparison process, voice tests were conducted and the quality between the baseline test and the clarity of the voice transmissions compared using the airborne relay node. Table 10 is a graphic depiction of the voice transmission comparison measures between the baseline test and the airborne relay node test.

Distances	Baseline	Airborne Relay Node
1 kilometer	Excellent/Good/Poor	Excellent/Good/Poor
2 kilometer	Excellent/Good/Poor	Excellent/Good/Poor
3 kilometer	Excellent/Good/Poor	Excellent/Good/Poor
4 kilometer	Excellent/Good/Poor	Excellent/Good/Poor

Table 10. Airborne Relay Node Voice Transmission Effectiveness Comparison Model

a. Test Distances

The test distances were selected based on approximations of how much terrain a dismounted small unit would cover in an Afghanistan or Iraq scenario. However, it is important to note these distances and times may vary depending on environmental conditions, such as mountainous versus urban terrain. The distances represent the best estimates taken from the author’s prior operational experience. Additionally, the

distances represent short duration vehicle convoys that may involve scenarios, such as battlefield circulation, key leader engagements, and re-supply missions to combat outposts. The range of distance over which most of these activities could potentially operate is between approximately one kilometer and four kilometers.

b. Throughput

Throughput can be defined as the minimum transmission rate along the path between source and destination. An example of how this process works is to consider two end systems, a server and client, transferring files over a communication link that can be considered a pipe and the file transferred as fluid going through the pipe. The quantity of "fluid" received at the "sink" over a given amount is the throughput rate and is measured in bits per second (bps.) (Kurose, 2010, p. 48). In this test, the Iperf network performance tool was used to gather throughput rates between Wave Relay™ nodes. Iperf provided statistical averages of throughput rates in both commonly used WLAN protocols TCP and UDP.

C. TESTS AND RESULTS

Prior to creating a formal test and demonstration, a informal test was conducted to ensure that the airborne radio payload selected would not affect the airworthiness of the Raven RQ 11B. The informal test was begun by checking the systems in static positions and clear LOS to ensure the communication link was not obstructed. The test started with voice transmission checks and it was possible to obtain a strong, clear signal with excellent clarity. An *Iperf* data network performance test was also conducted in which the goal was to ensure a two-way data communication between two end-systems. With the support of California National Guard, it was possible to deploy the systems at the Camp Roberts, CA training area and conduct an initial airborne relay feasibility test. Prior to launching the Small-UAS, the ground systems were confirmed to be masked by natural terrain and no communication links were attainable by conducting voice and data transmission checks; the terrain impeded any form communication. Next, the launched the Small-UAS was launched with the Wave Relay™ Single Board radio attached and it established an altitude of 1,500ft Mean Sea level (MSL). Once the Small-UAS launch

was established, the Raven RQ 11B operator began circular flight patterns above the ground nodes. The voice test was then conducted again and achieved two-way voice transmissions was successfully with excellent clarity. Simulated file transfers with *Iperf* were thus begun, and “files” were successfully sent from the server to the client. After confirming that the payload was supported by the Small-UAS and that a communication link was viable, a more formal test was pursued.

1. Voice Transmission Test and Results

After the informal test at Camp Roberts, CA, the formal test concept formulation was begun. It was decided to establish baseline tests, as before, to compare the results between point-to-point ground radios and the results obtained by using the airborne relay node. A scientific instrument was not available to measure the effectiveness and clarity of the voice links; instead, as mentioned previously, a subjective scale was generated using human end-user input on clarity-quality metrics.

a. Baseline Voice Test

The decision was made to conduct the baseline test in a field environment to reduce bias in the follow-on testing of the airborne relay node. A portion of the Salinas Valley, CA was chosen to conduct the test. Figure 15 is a Google Earth satellite image depicting the terrain where the baseline test was conducted. The vegetation in the image is mostly agricultural crops and small brush, and not trees crossing the LOS path. The two icons represent the ground stations and the green line between the icons represents the straight-line distance, which in this image, is the 2-kilometer test. As the image shows, this environment offered unobstructed LOS for the baseline voice transmission tests.

Figure 15. Google Earth™ Satellite Image of Baseline Test Area (From: Google Inc., 2012).

Prior to beginning the test, Quad Radios were set up to specific settings and recorded for future use with the airborne relay node test. Again, these measures were taken to reduce bias and provide the ability to replicate testing. The settings were configured using the Wave Relay™ Quad Radio Router graphic interface, which can be accessed via a personal computer. The Quad Radio channel bandwidth was set at 5 MHz, and the coverage area to 8.1 kilometers. Figure 16 is a screen shot of the Wave Relay™ Quad Radio Router graphic setting interface, which is very intuitive. Further explanation on the use and configuration of the Wave Relay™ Quad Radio can be found in Appendix C.

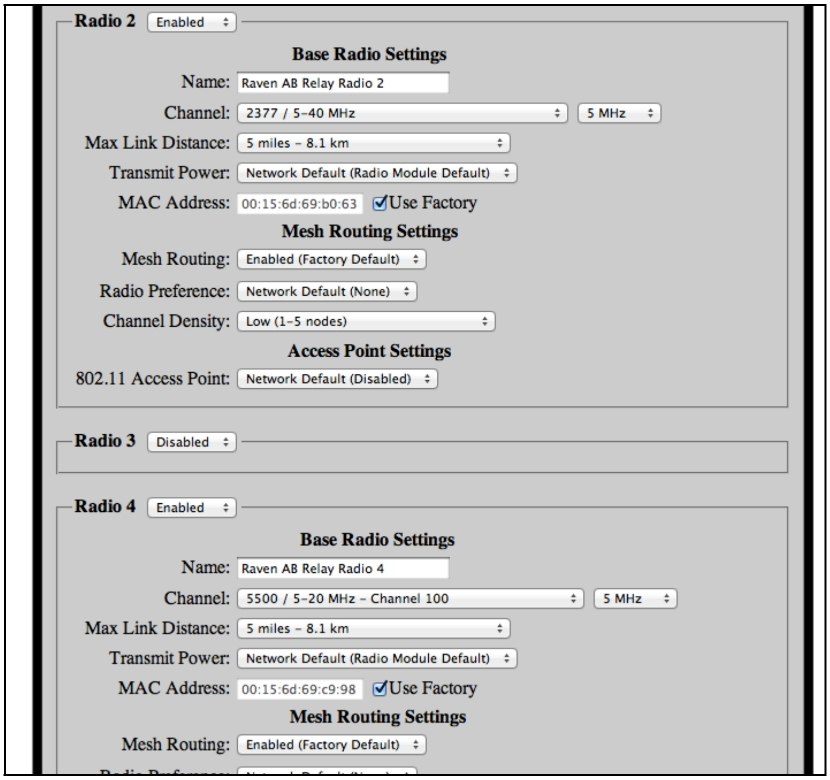


Figure 16. Wave Relay™ Quad Radio Graphic Settings Interface

Once the equipment was operational, the 1-kilometer two-way voice transmission test was begun. The sample size was set as $n = 5$ and subjectively rated the clarity of the voice transmissions. The same procedures were repeated for the 2-kilometer, 3-kilometer, and 4-kilometer tests. Table 11 provides a list of the measures of effectiveness (MOE) results for the baseline voice transmission test at each respective distance.

Distance	**Baseline Averages**
1 Km	Excellent
2 Km	Excellent
3 Km	Good
4 Km	Good

Table 11. Baseline Test Voice Transmission Results

b. Airborne Relay Node Voice Transmission Test

For the airborne relay test, the researchers returned to Camp Roberts, CA, with support from the California National Guard, which provided the Raven RQ 11B and operators, as well as the tactical ground vehicles and drivers. Similar to the informal test, a secure environment was created in which the masking terrain would obstruct the tactical radios' LOS. After ensuring the communication link between the two ground stations was unattainable, the Small-UAS was launched with the Wave Relay™ Single Board radio attached. The same sample sets of $n = 5$ were replicated for the pre-determined distances. The settings on the Wave Relay™ Quad Radio Router were identical to those of the baseline tests. It was not possible to obtain data for the 4-Kilometer airborne relay tests due to equipment failure; the battery powering the Wave Relay™ Single Board Radio was completely drained and it was not possible to recharge it. Table 12 provides a side-by-side comparison of the voice transmission results using the subjective scale.

Distance	**Baseline Test**	**Airborne Relay Test**
1 Km	Excellent	Excellent
2 Km	Excellent	Excellent
3 Km	Good	Excellent
4 Km	Good	No Test

Table 12. Measures of Effectiveness Voice Transmission Comparisons

c. Voice Transmission Observations

During the voice transmission tests, some observations were made that are noteworthy and may provide more granularity to the results. In the baseline test, it was noticed that at 3 kilometers, the voice transmissions had background noise. The signal remained strong but clarity began to degrade. Also noted was that the baseline tests were conducted during periods of strong winds. These environmental conditions may have attributed to the background noise.

2. Data Transfer Test and Results

The second task in the test procedure was to perform a data transfer comparison test. The steps were similar to the voice transmission set up, in which established a baseline test was first established in a semi-controlled environment and later side-by-side comparisons of those results were made with those of the airborne relay. A significant difference between the voice and data tests is that it was possible to use a quantitative measuring instrument to collect throughput transfer rates, thereby making the results for the data tests more objective in nature.

a. Data Transfer Baseline

The equipment set up and environmental conditions were the same as for the voice transmission tests. Based on inputs from the author's previous operational experiences, the file size was narrowed to 10MB. A 10 MB file represents the typical information set that would be sent over a network in tactical environment. Examples of the type of information being sent and received are satellite imagery, concept of operation slides with high-resolution graphics, and full motion video. *Iperf* simulates the file transfer from server to client and provides the network administrator with a throughput rate average for each communication session.

For the data transfer throughput, a sample size of $n = 50$ was selected, which is greater than a sample size of 30 that allowed the use of the normal distribution as an approximation for the sampling distribution, $\overline{X}$, in accordance with the Central Limit Theorem (Keller, 2008, p. 300). Thus, 50 iterations of a simulated file transfer of 10 MB were performed for each respective distance. *Iperf* provided averages of throughput rates for each sample. Figure 17 is a screen shot of the graphical version of *Iperf*, known as *Jperf*, which depicts the settings used and the outputs provided by the software. The *Iperf* outputs were recorded used Microsoft Excel to compute the mean for the sample set of $n = 50$ for each respective distance. Table 13 lists the mean values for the baseline test throughput rates in megabit per second (Mbps.)

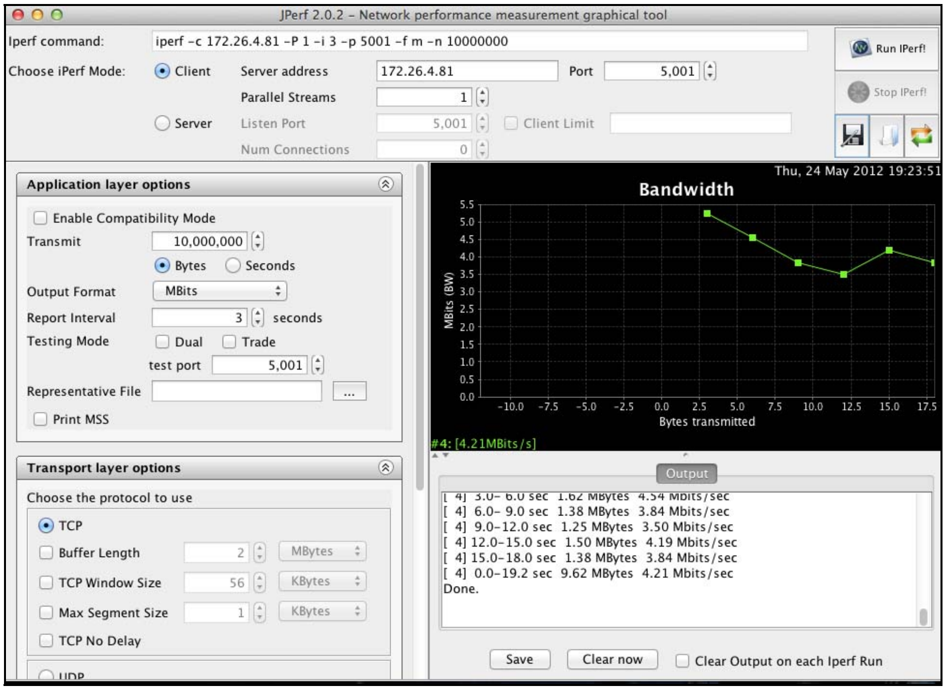


Figure 17. *Iperf/JPerf* Network Performance Tool Baseline Throughput Rate Test

Distance	TCP	UDP
1 Km	$\mu = 8.15 Mbps$	$\mu = 8.38 Mbps$
2 Km	$\mu = 8.25 Mbps$	$\mu = 9.68 Mbps$
3 Km	$\mu = 8.19 Mbps$	$\mu = 8.57 Mbps$
4 Km	$\mu = 8.17 Mbps$	$\mu = 9.54 Mbps$

Table 13. TCP and UDP Baseline Test Data Throughput Averages

b. Data Rate Baseline Test Observations

No great abnormalities, other than data rates were greater at the 2 Km mark, were observed during the baseline test. All communication links were point-to-point and the equipment settings were identical for each test. The only rational explanation is perhaps environmental conditions may have caused a slight difference in rates. The 2 Km test was conducted at night and the others during daytime hours, which may have resulted in a better signal-to-noise ratio for the 2Km-test, as the noise floor for the night environment may have been lower. The researchers did not measure this, however.

c. Data Transfer Airborne Relay Node

For the airborne relay vertical network node tests, the same procedures were repeated for the data tests as for the voice transmission tests at Camp Roberts. The equipment settings were identical to the baseline test and sample the size was also $n = 50$ for each test at the respective distances. As mentioned earlier, equipment failure limited the amount of data that could be gathered for the airborne relay test. Therefore, the final comparison model will not have side-by-side comparisons for each distance set out to be captured. However, sufficient information was collected to build the statistical model and assess the hypothesis of this thesis. Table 14 reports the computed effective data rate averages of the airborne vertical node test.

Distance	**TCP**	**UDP**
1 Km	$\mu = 1.39 Mbps$	$\mu = 0.18 Mbps$
2 Km	$\mu = 2.00 Mbps$	$\mu = 0.09 Mbps$
3 Km	$\mu = 1.31 Mbps$	No Test
4 Km	No Test	No Test

Table 14. TCP and UDP Airborne Relay Data Throughput Averages

d. Airborne Relay Node Observations

The airborne node performance averages were significantly lower than the point-to-point ground tests, which contradicted the going-in assumptions. A possible explanation for this occurrence is the fact that the data had to travel two hops to reach its final destination, versus the single-hop point-to-point ground network. This finding is significant in that the UAV only had the single radio. Thus, its time workload was split between receiving and transmitting, thus effectively halving the available capacity. The other critical factor is that the payload mounted onto the aircraft is not specifically designed to perform a communication relay. Payload components were taped to the fuselage to include the antenna. The taped antenna probably moved in flight, which caused pointing variations. Also noted was that data rates were higher when the Small-UAS was directly overhead the ground nodes.

3. Comparison Models and Analysis

The final step in the test series was to compile and analyze the results using statistical models to demonstrate MOE of both the baseline test and the airborne relay node tests. Are going-in assumption was a Small-UAS, controlled by the forward deployed mobile unit (platoon/squad or below), would not provide tactical data communication link benefit to the dismounted or mobile mission element. The baseline test averages were used as desired measures of effectiveness. A statistical hypothesis test was generated to say statistically whether the airborne relay could or could not provide data connectivity at rates at or close to the baseline tests. The following are the computations for the first hypothesis test, in which the mean of the baseline test is assumed to be equal to the airborne relay test.

Based on the computations, the null hypothesis is rejected. It was confirmed that statistically a Small-UAS airborne relay could provide a tactical data communication link; however, the throughput rates were well below the baseline throughput rates. For the 1 Km TCP tests, a manual set up of how the statistic was framed was provided. For the remaining TCP tests, Excel outputs were used. The same Excel steps were repeated to compute the UDP 1 Km and 2 Km tests. All the p-values returned with 0%, confirming that the airborne relay throughput rates performance were below the baseline means. Although statistically the airborne relay did not match the baseline rates, the null hypothesis that airborne relay cannot provide data connectivity to small military units in communication-degraded environments is rejected. Figure 18 depicts the step-by-step manual process of computing the 1 Km TCP null hypothesis test and the Excel outputs.

1 Km TCP Null Hypothesis Test

$H_0 : Baseline\mu = Airborne\mu$
$H_1 : Baseline\mu \neq Airborne\mu$

Baseline	Airborne
$\mu = 8.16 Mbps$	$\mu = 1.39 Mbps$
$\sigma = .19$	$\sigma = .53$

Student T Test Formula

$$t = \frac{\overline{X}_1 - \overline{X}_2}{\sqrt{\frac{S_1^2}{n_1} + \frac{S_2^2}{n_2}}} = \frac{8.16 - 1.30}{\sqrt{\frac{.19^2}{50} + \frac{.53^2}{50}}}$$

T Test = 85.17
P-Value = 0.00

TCP Throughput Null Hypothesis	Baseline 1 km	Airborne 1 Km	Baseline 2km	Airborne 2km	Baseline 3 km	Airborne 3 Km
Average	8.16	1.39	8.25	2.00	8.19	1.31
Standard Deviation	0.19	0.53	0.03	0.77	0.07	0.38
Test Statistic		85.17		57.06		174.38
P-Value		0.00		0.00		0.00

UDP Throughput Null Hypothesis	Baseline 1 km	Airborne 1 Km	Baseline 2km	Airborne 2km
Average	8.38	0.18	9.68	0.09
Standard Deviation	2.75	0.41	1.03	0.15
Test Statistic		20.85		65.05
P-Value		0.00		0.00

Figure 18. 1 Km TCP Null Hypothesis Computation and Excel Produced Results for Additional Distance and UDP Tests

These statistics should not be considered a refuting of the value of the airborne relay and its functionality. In a communication-degraded environment, the airborne relay would mean a communication link versus no communication link. Figure 19 provides graphs depicting side-by-side throughput rate comparisons between the TCP baseline test and airborne relay test; Figure 20 depicts the UDP portion of the tests.

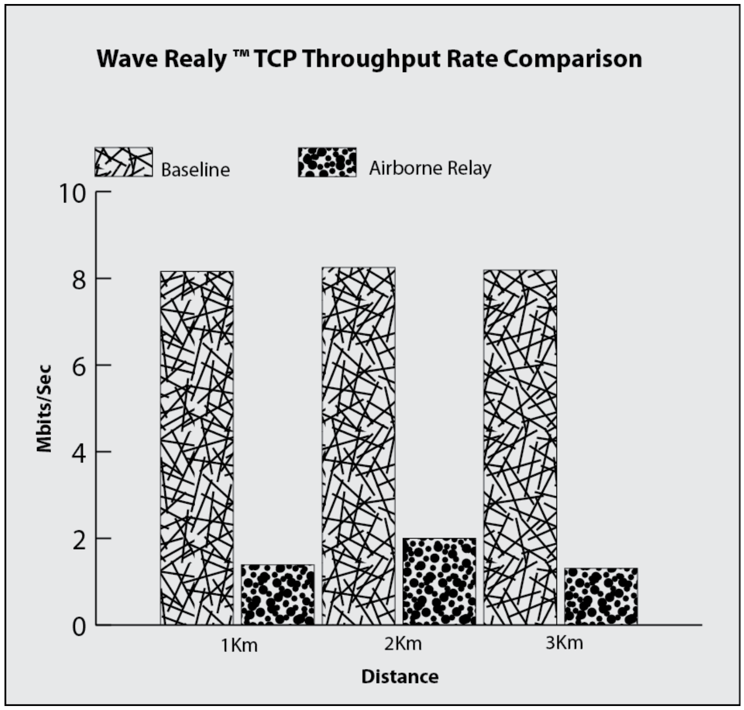


Figure 19. TCP Data Throughput Rate Comparisons Between Baseline Test and Airborne Relay Node Test

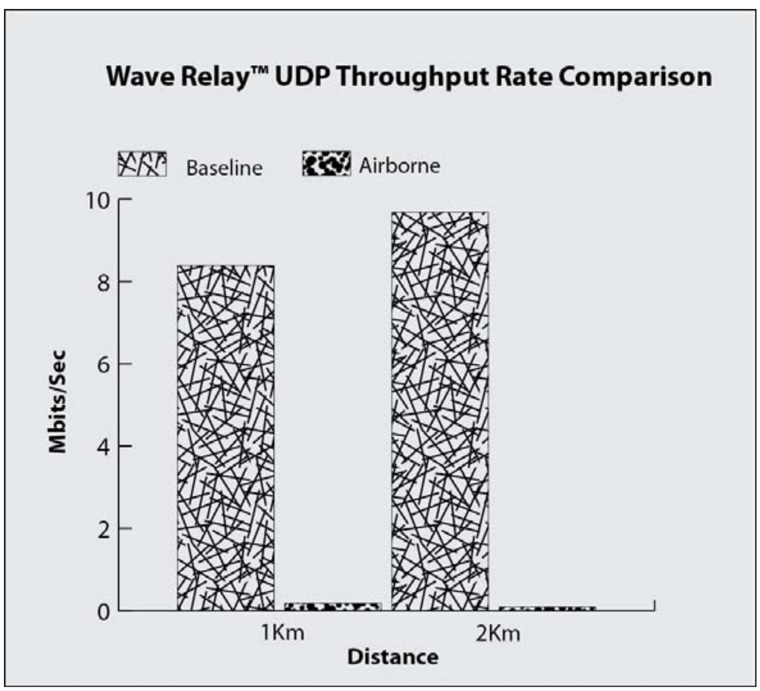


Figure 20. TCP Data Throughput Rate Comparisons Between Baseline Test and Airborne Relay Node Test

4. Small-UAS Network Node Operations

For the test, none of the normal Raven RQ 11B physical airframe integrity was altered; nor did the addition of the externally mounted radio compromise its airworthiness. The communication payload weighed approximately .25lbs and was taped to the fuselage. However, the additional weight did degrade the endurance of the Small-UAS. The average flight time from the fully charged battery is 90 minutes, with the external payload the flight time being reduced by 50%, which only provided 45 minutes of on-station time. Aside from the endurance time being decreased by 50%, no other observations were made that would indicate that the Small-UAS could not perform a multi-mission functionality.

D. SUMMARY

Overall, the researchers believe the tests and data gathered to prove the concept were a success. The RoIP results exceeded expectations and they are confident that voice C2 would be enhanced in a communication-degraded environment. The data throughput rates for the airborne rely did not meet the going-in assumptions; however, they are cognizant that the test bed equipment was ad hoc and not designed to perform communication relay function, particularly, the limitation of a single radio on the UAV performing both receive and send functions (i.e., half-duplex, store-and-forward relay). The next chapter discusses final conclusions and recommendations for future work in the field of Small-UAS based airborne relay nodes. The researchers are confident that further research will provide a highly integrated, deployable system with better throughput rates, endurance time and significantly improved communication links in environments that lack fixed infrastructure.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND FUTURE RESEARCH

A. CONCLUSIONS

Based on the equipment tested, it was shown the Wave Relay™ Single Board Radio integrated with the Raven RQ 11B Small-UAS could provide a tactical networking solution that can improve both voice transmissions and data transfers using TCP/IP protocols in communication degraded environments. The Small-UAS airborne relay platform can be used to extend tactical networks in masked terrain providing BLOS and persistent on-the-move communications to small mobile military units.

1. Communication Payload

The Wave Relay™ Single Board radio performed well alongside the Raven RQ 11B. No frequency interferences were detected between the frequencies used to operate the Small-UAS, nor was the ISR full motion video-feed frequency affected. It was observed that the single radio system was overwhelmed by having to both transmit and receive (i.e., relay) that caused delays and low throughput rates. Also noted was that the airborne relay system could benefit from a second radio to operate in a full duplex mode; thereby, increasing performance.

2. Small-UAS Airborne Relay

The Raven RQ 11B platform was used for the tests and field demonstration to emphasis re-use concepts and promote a cost-effective measure to address tactical communication inadequacies in periods of budget constraints. The Raven RQ 11B platform has been in military operation for three years and it is considered a workhorse in the Tier I category of UAV's. The Raven RQ 11B performance during the testing was exceptional and attested that it has the potential to become a multi-mission Small-UAS platform. However, the flight endurance was affected by the additional .5lbs weight put on the fuselage that reduced flight time by 50% (90 minute to 45 minutes). A vehicle-on-the-move test was performed and the operator had no issues controlling the UAV from moving vehicles and maintaining persistent on-the-move communications. However,

there was not sufficient time to perform a dismounted patrol and verify how the Small-UAS airborne relay system would impact a dismounted patrol when adding logistical considerations associated with the system.

B. FUTURE RESEARCH

While the ad hoc airborne relay radio configuration was adequate to demonstrate that a Small-UAS could perform a multi-mission function, and provides a communication link to small mobile units in a communication degraded environment, further refinement is required. Adding a payload not specifically designed to integrate with the Raven RQ 11B system reduced endurance time. Future research and collaboration may be required to engineer an adaptive modular payload that will seamlessly integrate with the Raven RQ 11B and not impact optimal performance. Ideally, the communication payload design would seamlessly integrate by embedding it in the nosecone of the aircraft, and power for the radios would be drawn from the aircraft's main power source. Also, in an effort to pursue a cost effective solution or interoperable capability, further research should be conducted with respect to introducing a GOTS payload.

The tests and demonstrations were intended to validate that the Small-UAS airborne relay can perform as a possible solution for providing small mobile units with a communication link in masked terrain and while on the move. To measure the effectiveness of the airborne relay, a baseline throughput rate was established using a point-to-point topology. The throughput rates were used as best-case scenarios. Further research and comparison trials are recommended in this area to compare the measures of performance between the use of a ground and airborne relay using TCP/IP protocols. In Appendix E , all of Ipref data outputs and Excel models are included that can benefit future researchers conducting comparison models of throughput rates between ground and airborne relays.

While it was successfully validated that the small-UAS airborne relay can provide BLOS and on-the-move communication links, further research is recommended with a focus placed on the introduction of multiple airborne relay nodes. The introduction of multiple airborne relays can potentially extend the range and duration times of the tactical networks.

Also, the research introducing multiple UAVs to create mesh networks should consider the employment of autonomous UAV systems, which could eliminate the need for operator crews and reduce the logistical footprint that might burden a small tactical unit. The logistical burdens include the weight of batteries and the ground station equipment required to fly and maintain positive control of the aircraft. The use of autonomous UAVs can also eliminate the need for an operator crew, which consists of two personnel. Such personnel must be formally trained and log flight hours to maintain technical proficiency, which could potentially detract from performing primary duties.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. TEST AND DEMONSTRATION PRELIMINARY WORK

Major Jose Menjivar
NPS Wireless Research Group
Tactical Network Topology Experimentation
Camp Roberts, Army National Guard Base
February 2012

TRIP REPORT

Initial Proof of Concept: Small UAS Tactical Airborne Relay

Test Participants:

- Team Lead: Major Jose Menjivar, NPS Information Technology Student
- Senior Systems Engineer: Charles Prince, NPS Staff
- Systems Engineer: Aurelio Monarrez, NPS Staff and Student
- Raven 11B Crew: Sergeant Timothy Fisher, A-Troop 1-18 CAV, USANG, Specialist Michael V. Wilson C-Troop 1-18 CAV, USANG
- Facilitator: Professor John Gibson, NPS Computer Science Dept.

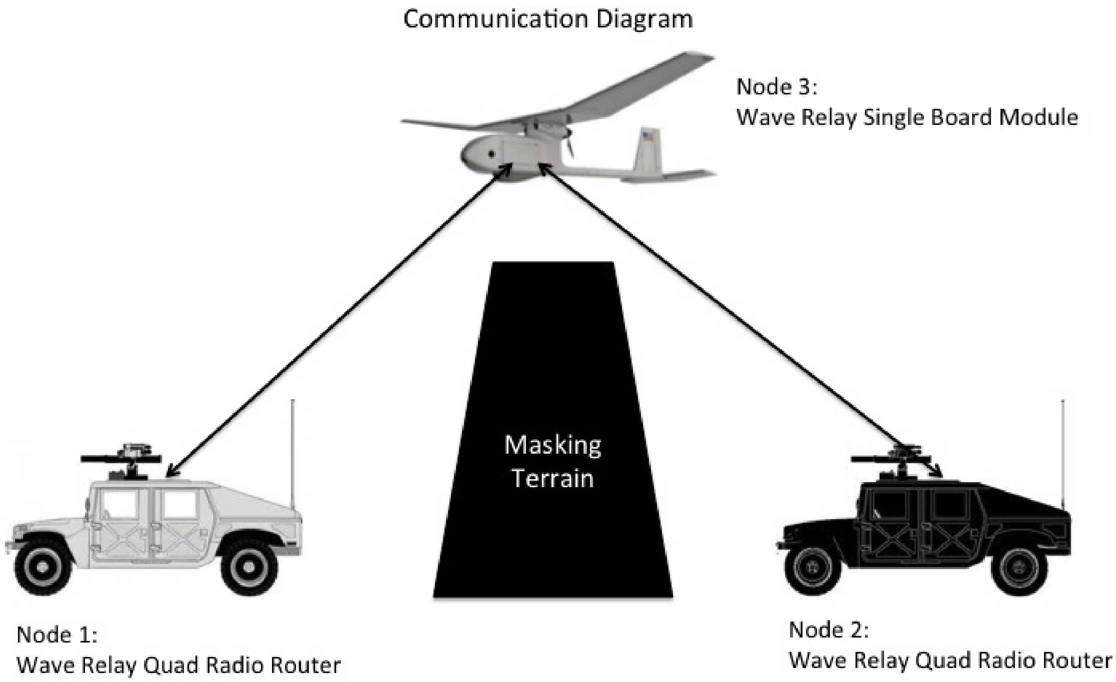
Objectives:

- Conduct non-intrusive modifications to Raven 11B by adding a Wave Relay Single Board Module communication payload, power source, and omni-directional antenna to Small UAS. This modification will enable Small UAS to act as an airborne tactical communications relay station.
- Conduct initial static point-to-point relay tests with Raven 11B Small UAS airborne relay station and Wave Relay Quad Router Radio Systems
- Confirm Small UAS airborne relay station can enable static beyond line sight of tactical communications
- Confirm Small UAS airborne relay station equipped with Wave Relay Single Board Module can transmit voice communications beyond line of sight within three nodes that are masked by terrain

- Confirm Small UAS airborne relay station equipped with Wave Relay Single Board Module can transmit data packets beyond line of sight within three nodes that are masked by terrain

Test Environment:

- Node 1: HMMWV M1114 Tactical Vehicle equipped with proprietary Wave Relay Quad Radio Router System
    - Location: Stationary position approximately 2.5 kilometers away from node 2, line of sight was intentionally obstructed by masking terrain to prove beyond line of sight concept
- Node 2: HMMWV M1114 Tactical Vehicle equipped with proprietary Wave Relay Quad Radio Router System
    - Location: Stationary position approximately 2.5 kilometers away from node 1, line of sight was intentionally obstructed by masking terrain to prove beyond line of sight concept
    - See enclosure 1.
- Node 3: Aerovironment Raven 11B non-intrusive modifications that include the use of proprietary Wave Relay Single Board Module encased in cardboard box and weather proofed with a plastic bag and placed on fuselage with non-stick tape. The proprietary Wave Relay Single Board Module was powered by Thunder Power Lithium Polymer 65C 2250mAh 3-cell battery, which was also taped to fuselage. An omni-directional antenna was taped to bottom of fuselage. The weight of the payload was approximately .7 pounds. When placing payload on Small UAS aerodynamics and weight constraints were taken into consideration. To reduce impact on the integrity of the airframe the team carefully selected areas to place payload to ensure there was counter balance and even weight distribution. The team taped down extraneous parts to create better aerodynamics and mitigate loss of flight endurance.
    - Location: The Raven 11B crew was located approximately 2 kilometers from node 1 and 1.5 kilometers from node 2. Once the Small UAS was airborne it climbed to 400 AGL (1200 MSL), and conducted circular flight patterns around nodes 1 and 2.
    - See enclosure 2.



Test:

Team deployed node 2 and node 3 to training areas within Camp Roberts. Node 2 occupied static location behind a terrain feature large enough to mask line of sight communication capability with node 2. Node 2 was in placed behind terrain a voice communication check was attempted without the use of airborne relay. The masking terrain impeded voice transmission and also prevented from node 1 from tracking nodes 2 and 3 on the digital network. Once it was concluded that line sight communication was not feasible the team launched Node 3 (Raven 11B airborne relay.) The Raven operator launched the aircraft and noticed a slight wobble due added weight. The operator reported the aircraft corrected itself once sufficient airlift was gained. The Small UAS climbed to 400 AGL (1200MSL) was established at set altitude the team conducted a voice communication test between node 1 and 2 relayed through node 3. The voice test was successful and transmissions were heard with high quality of service and low transmission latency. The follow on test was transmission of data packets simulating transfer of data files. The test began with small packets being transferred and

incrementally increased in size (enclosure 3.) All data transfers transmitted by node 1 were received by node 2.

Findings: The field test proved the concept that airborne relay can enable beyond line of sight communications, both voice and data transmissions. At 400 AGL the airborne relay was able to provide a 2-kilometer radius communication area. The test also captured the quality of service and transfer rates improved when aircraft was directly overhead of ground nodes.

Any questions please contact team leader:

Major Jose Menjivar
Information Technology Management
jdmenjiv@nps.edu

(Enclosure 1)

Wave Relay Quad Radio Router System Mounted M1114

(Enclosure 2)

Wave Relay Single Board Module Mounted on Raven 11B

Iperf Throughput Averages Data transfer Report:

Server listening on TCP port 5001

TCP window size: 256 KByte (default)

----

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50151

[ID] Interval Transfer Bandwidth

[4] 0.0-11.3 sec 896 KBytes 647 Kbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50152

[5] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50153

[4] 0.0-15.8 sec 256 KBytes 133 Kbits/sec

[5] 0.0-46.5 sec 512 KBytes 90.3 Kbits/sec

[SUM] 0.0-46.5 sec 768 KBytes 135 Kbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50155

[5] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50164

[5] 0.0-150.3 sec 256 KBytes 14.0 Kbits/sec

[5] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50165

[4] 0.0-174.8 sec 896 KBytes 42.0 Kbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50166

[5] 0.0-232.8 sec 1.12 MBytes 40.5 Kbits/sec

[4] 0.0-548.7 sec 256 KBytes 3.82 Kbits/sec

[SUM] 0.0-548.7 sec 2.50 MBytes 38.2 Kbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50182

[4] 0.0-10.5 sec 2.12 MBytes 1.69 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50183

[4] 0.0-11.3 sec 2.12 MBytes 1.58 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50184

[4] 0.0-10.4 sec 3.25 MBytes 2.62 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50185

[4] 0.0-11.4 sec 1.88 MBytes 1.38 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50186

[4] 0.0-10.4 sec 3.75 MBytes 3.01 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50187

[4] 0.0-10.8 sec 3.12 MBytes 2.43 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50188

[4] 0.0-12.0 sec 1.62 MBytes 1.14 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50189

[4] 0.0-13.0 sec 1.75 MBytes 1.13 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50190

[4] 0.0-13.9 sec 1.62 MBytes 979 Kbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50191

[4] 0.0-11.0 sec 512 KBytes 382 Kbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50198

[4] 0.0-10.7 sec 1.25 MBytes 982 Kbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50199

[4] 0.0-11.6 sec 1.38 MBytes 999 Kbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50200

[4] 0.0-10.4 sec 2.62 MBytes 2.11 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50201

[4] 0.0-10.3 sec 3.75 MBytes 3.04 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50202

[4] 0.0-11.0 sec 3.00 MBytes 2.29 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50203

[4] 0.0-11.1 sec 2.25 MBytes 1.70 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50204

[5] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50205

[4] 0.0-15.3 sec 1.38 MBytes 756 Kbits/sec

[5] 0.0-25.5 sec 768 KBytes 247 Kbits/sec

[SUM] 0.0-25.5 sec 2.12 MBytes 700 Kbits/sec

^C

sh-3.2#

sh-3.2# cat /Users/jdmenjivar1971/iperf

iperf iperf.log1

sh-3.2# cat /Users/jdmenjivar1971/iperf.log1

Server listening on TCP port 5001

TCP window size: 256 KByte (default)

----

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50151

[ID] Interval Transfer Bandwidth

[4] 0.0-11.3 sec 896 KBytes 647 Kbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50152

[5] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50153

[4] 0.0-15.8 sec 256 KBytes 133 Kbits/sec

[5] 0.0-46.5 sec 512 KBytes 90.3 Kbits/sec

[SUM] 0.0-46.5 sec 768 KBytes 135 Kbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50155

[5] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50164

[5] 0.0-150.3 sec 256 KBytes 14.0 Kbits/sec

[5] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50165

[4] 0.0-174.8 sec 896 KBytes 42.0 Kbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50166

[5] 0.0-232.8 sec 1.12 MBytes 40.5 Kbits/sec

[4] 0.0-548.7 sec 256 KBytes 3.82 Kbits/sec

[SUM] 0.0-548.7 sec 2.50 MBytes 38.2 Kbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50182

[4] 0.0-10.5 sec 2.12 MBytes 1.69 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50183

[4] 0.0-11.3 sec 2.12 MBytes 1.58 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50184

[4] 0.0-10.4 sec 3.25 MBytes 2.62 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50185

[4] 0.0-11.4 sec 1.88 MBytes 1.38 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50186

[4] 0.0-10.4 sec 3.75 MBytes 3.01 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50187

[4] 0.0-10.8 sec 3.12 MBytes 2.43 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50188

[4] 0.0-12.0 sec 1.62 MBytes 1.14 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50189

[4] 0.0-13.0 sec 1.75 MBytes 1.13 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50190

[4] 0.0-13.9 sec 1.62 MBytes 979 Kbits/sec

```
[ 4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50191
[ 4] 0.0-11.0 sec 512 KBytes 382 Kbits/sec
[ 4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50198
[ 4] 0.0-10.7 sec 1.25 MBytes 982 Kbits/sec
[ 4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50199
[ 4] 0.0-11.6 sec 1.38 MBytes 999 Kbits/sec
[ 4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50200
[ 4] 0.0-10.4 sec 2.62 MBytes 2.11 Mbits/sec
[ 4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50201
[ 4] 0.0-10.3 sec 3.75 MBytes 3.04 Mbits/sec
[ 4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50202
[ 4] 0.0-11.0 sec 3.00 MBytes 2.29 Mbits/sec
[ 4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50203
[ 4] 0.0-11.1 sec 2.25 MBytes 1.70 Mbits/sec
[ 4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50204
[ 5] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50205
[ 4] 0.0-15.3 sec 1.38 MBytes 756 Kbits/sec
[ 5] 0.0-25.5 sec 768 KBytes 247 Kbits/sec
[SUM] 0.0-25.5 sec 2.12 MBytes 700 Kbits/sec
sh-3.2#
sh-3.2# cat /Users/jdmenjivar1971/iperf.log1
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 256 KByte (default)
------------------------------------------------------------
[ 4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50151
[ ID] Interval Transfer Bandwidth
[ 4] 0.0-11.3 sec 896 KBytes 647 Kbits/sec
[ 4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50152
[ 5] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50153
```

[4] 0.0-15.8 sec 256 KBytes 133 Kbits/sec

[5] 0.0-46.5 sec 512 KBytes 90.3 Kbits/sec

[SUM] 0.0-46.5 sec 768 KBytes 135 Kbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50155

[5] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50164

[5] 0.0-150.3 sec 256 KBytes 14.0 Kbits/sec

[5] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50165

[4] 0.0-174.8 sec 896 KBytes 42.0 Kbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50166

[5] 0.0-232.8 sec 1.12 MBytes 40.5 Kbits/sec

[4] 0.0-548.7 sec 256 KBytes 3.82 Kbits/sec

[SUM] 0.0-548.7 sec 2.50 MBytes 38.2 Kbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50182

[4] 0.0-10.5 sec 2.12 MBytes 1.69 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50183

[4] 0.0-11.3 sec 2.12 MBytes 1.58 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50184

[4] 0.0-10.4 sec 3.25 MBytes 2.62 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50185

[4] 0.0-11.4 sec 1.88 MBytes 1.38 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50186

[4] 0.0-10.4 sec 3.75 MBytes 3.01 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50187

[4] 0.0-10.8 sec 3.12 MBytes 2.43 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50188

[4] 0.0-12.0 sec 1.62 MBytes 1.14 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50189

[4] 0.0-13.0 sec 1.75 MBytes 1.13 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50190

[4] 0.0-13.9 sec 1.62 MBytes 979 Kbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50191

[4] 0.0-11.0 sec 512 KBytes 382 Kbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50198

[4] 0.0-10.7 sec 1.25 MBytes 982 Kbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50199

[4] 0.0-11.6 sec 1.38 MBytes 999 Kbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50200

[4] 0.0-10.4 sec 2.62 MBytes 2.11 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50201

[4] 0.0-10.3 sec 3.75 MBytes 3.04 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50202

[4] 0.0-11.0 sec 3.00 MBytes 2.29 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50203

[4] 0.0-11.1 sec 2.25 MBytes 1.70 Mbits/sec

[4] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50204

[5] local 192.168.113.13 port 5001 connected with 192.168.113.11 port 50205

[4] 0.0-15.3 sec 1.38 MBytes 756 Kbits/sec

[5] 0.0-25.5 sec 768 KBytes 247 Kbits/sec

[SUM] 0.0-25.5 sec 2.12 MBytes 700 Kbits/sec

sh-3.2#

(Enclosure 3)

Major Jose Menjivar
NPS Wireless Research Group
Tactical Network Topology Experimentation
Camp Roberts, Army National Guard Base
March 2012

May 2012 Planning and Experiment Requirements

Proof of Concept: Small UAS Tactical Airborne Relay

Test Participants:

- Team Lead: Major Jose Menjivar, NPS Information Technology Student
- Senior Systems Engineer: Charles Prince, NPS Staff
- Systems Engineer: Aurelio Monarrez, NPS Staff and Student
- Raven 11B Crew: TBD
- Facilitator: Professor John Gibson, NPS Computer Science Dept.

Pre-Tactical Network Topology Experimentation Objectives:

- Conduct static test at Naval Post-Graduate School prior to May 2012 Tactical Network Topology (TNT) Experimentation. The purpose for conducting tests prior to TNT is to gather data in a structured environment and establish baselines. The tests will be conducted using the Wave Relay Quad Router Relay communication system. These baselines are measurements of voice transmission latency using Radio Over IP, OFMD with Adaptive Modulation Algorithm, and wireless data transfer throughput using 802.11 a/b/g/ Access Point management concurrent with Mobile Ad-hoc Network. The Wave Relay Quad Router Radio system does not differentiate between voice or data transmissions, therefore voice round trip time latency and data throughput can be measured by using the Ipref open source software application network-measuring tool. Ipref has been designed to assist network engineers capture the flow of data between to network nodes. The test will be performed under defined parameters. As a method of control defined distances and no variation in equipment will be implemented. This is an attempt to eliminate bias and create conditions were the tests can be replicated in the future. Voice and data streaming tests will be point-to-point at straight-line distances of 1 kilometer, 2 kilometers, 3 kilometers, and 4 kilometers.

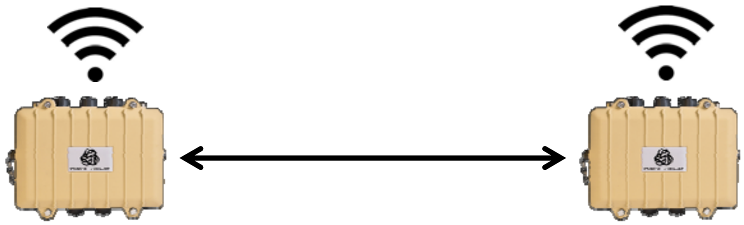


Figure 1: Straight line Point-to-Point Static Tests at 1km, 2km, 3km, and 4km.

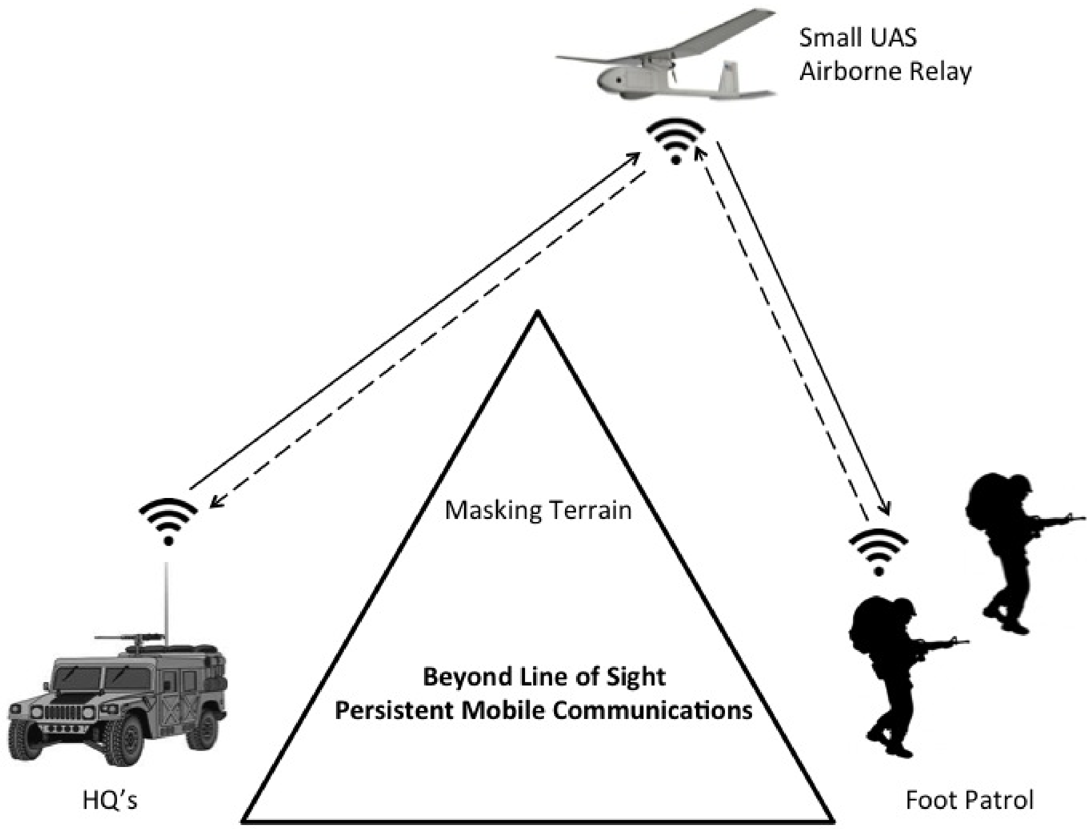
TNT Objectives:

- Conduct non-intrusive modifications to Raven 11B by adding a Wave Relay Single Board Module communication payload, power source, and omni-directional antenna to Small UAS. This modification will enable Small UAS to act as an airborne tactical communications relay station.
- Conduct point-to-point relay tests with Raven 11B Small UAS airborne relay station and Wave Relay Quad Router Radio Systems during a foot mobile patrol and vehicle-mounted patrol.
- Confirm Small UAS airborne relay station can enable beyond line of sight and persistent tactical communications of both voice and data transmissions while a foot mobile patrol is on the move at distances ranging from 1km to 4km radius.
- Confirm Small UAS airborne relay station can enable beyond line of sight and persistent tactical communications of both voice and data transmissions while a vehicle-mounted patrol is on the move at distances ranging from 1km to 4km radius.

Test Requirements:

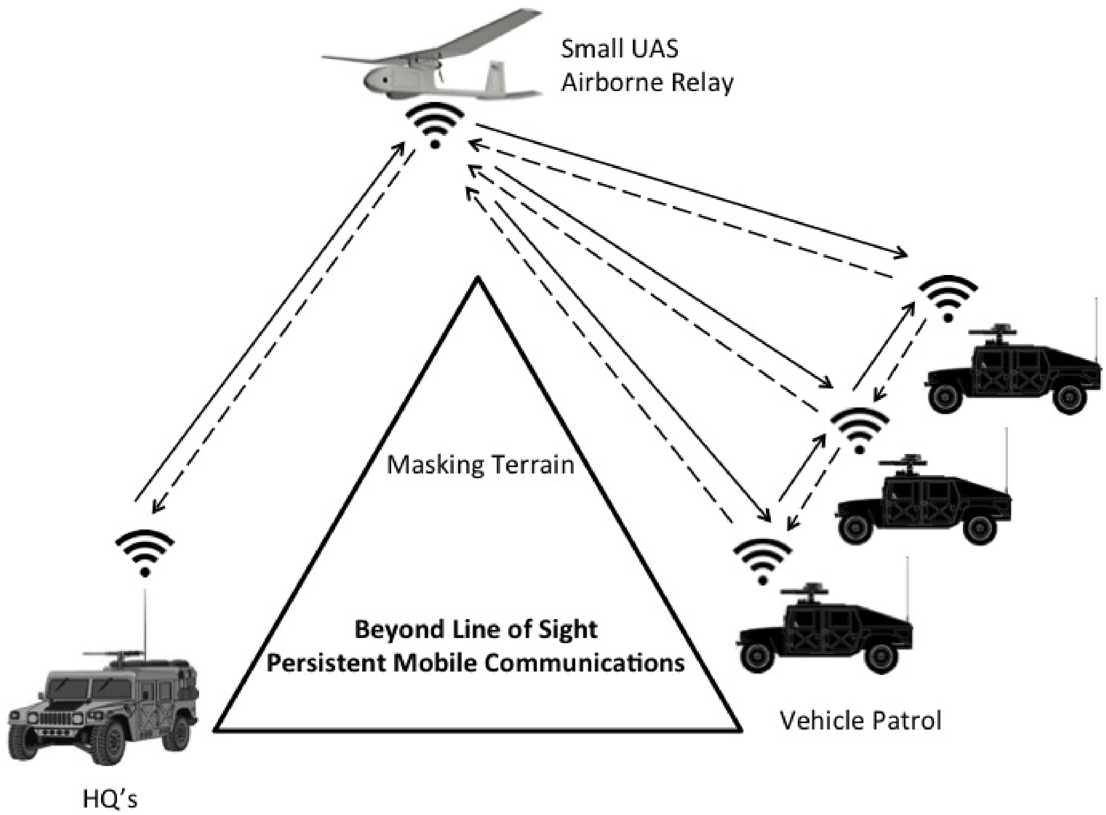
- Training area aboard Camp Roberts, CA the covering a 4km radius.
- Airspace aboard Camp Roberts to fly to Raven 11B, establish a ROZ with a 9000 MSL ceiling with a 4km radius.
- 1 Raven 11B crew, (1) Raven 11B Aircraft, (1) Raven 11B operator, and (1) Raven 11B pilot.
- Personnel support to simulate a foot mobile patrol. A minimum of 4 with the ability to carry (1) Wave Ralay Quad Router Radio, carry (1) laptop to capture data.
- Request for (3) HMMWV M1114 Tactical Vehicle equipped with proprietary Wave Relay Quad Radio Router Systems.
- Request for (3) HMMWV M1114 Tactical Vehicle drivers.

Concept of Operation 1: On the Move Foot Patrol



Deploy a foot patrol and Raven 11B crew into Camp Roberts, CA training area. Once the foot patrol is 1 km away from the command post and completely masked by terrain the patrol will launch Raven 11B Small UAS equipped with the Wave Relay Single Board Module. When the Raven 11B has gained 1200 MSL in altitude testing will begin. The first portion of test will be a voice transmission test while foot patrol is on the move. The latency time of the voice transmission will be captured with the use of Ipref software. At the conclusion of voice test, the team will begin data transfer test. Data packets will be transferred via two laptops. One laptop will be placed inside a patrol pack as a server, and the second laptop will be located at the command post set up as a client. The packets transferred will be incrementally increased in size and transfer rates will be captured using Ipref. The tests will be repeated three more times at distances of 2km, 3km, and 4km. The test will include testing quality of service with the increase of the Raven 11B altitude. The altitudes will range from 1200 MSL to 9000 MSL.

Concept of Operation 2: On the Move Vehicle Mounted Patrol



Deploy a vehicle patrol and Raven 11B crew into Camp Roberts, CA training area. Once vehicle mounted patrol is 1 km away from the command post and completely masked by terrain the patrol will launch Raven 11B Small UAS equipped with the Wave Relay Single Board Module. When Raven 11B has gained 1200 MSL in altitude testing will begin. The first portion of test will be a voice transmission test while vehicle-mounted patrol is on the move. The latency time of the voice transmission will be captured with the use of Ipref software. At the conclusion of voice test, the team will begin data transfer test. Data packets will be transferred via two laptops. One laptop will be placed inside one of the patrol vehicles as a server, and the second laptop will be located at the command post set up as a client. The packets transferred will be incrementally increased in size and transfer rates will be captured using Ipref. The tests will be repeated three more times at distances of 2km, 3km, and 4km. The test will include testing quality of service with the increase of the Raven 11B altitude. The altitudes will range from 1200 MSL to 9000 MSL.

Any questions please contact team leader:
Major Jose Menjivar
Information Technology Management
jdmenjiv@nps.edu

Naval Post-Graduate School Wireless Military Communications Research Group Testing and Experimentation, May 17-18, Camp Roberts, CA

Concept of Operations:

Purpose
The purpose of the event is to continue to explore and prove theories developed by NPS students, professors and partners. The results collected will generate data for thesis work and potentially develop wireless technology that will provide function and utility in real world applications.

Method
The Wireless Military Communication Research Group will coordinate with National Guard Unit in charge of operations and training aboard Camp Roberts to reserve training areas and airspace for testing. Research Group participants will coordinate individual travel and lodging. Participants will ensure requests for training areas, non-organic equipment, and non-organic personnel are submitted NLT 201700UAPR2012. Once at Camp Roberts the Research Group will begin testing NLT 170800UMAY2012 and conclude testing NLT 181700UMAY2012.

End-state
The Research Group's end-state is to conduct a safe and productive testing evolution. It is also the Research Group's desire to make the event effective and efficient to make good use of our time and that of our partners.

Coordinating Instructions:

1. Camp Roberts Operations and Training

a. Reserve training areas that encompass a 6-kilometer radius for foot mobile patrols.

b. Coordinate the allocation of (12) soldiers to participate in foot patrol experiment.

c. Point of Contact: SFC Richard G. Douthit, NG NGB richard.douthit@us.army.mil

2. NPS Wireless Military Communications Research Group

a. Submit all testing and experiment requirements NLT 281700UAPR2012.

b. Submit travel forms NLT 051700UMAY2012.

c. Coordinate special requirements or purchases with Professor John Gibson.

d. Conduct equipment operational checks at NPS several days prior to event. POC: Joseph Rivera jriver1@nps.edu.

e. Points of Contact: Professor John Gibson, 831-656-2902, jhgibson@nps.edu, Captain Joseph Rivera jriver1@nps.edu.

<u>3. Scheme of Maneuver</u>

A. **Voice Mesh Experiment:** This experiment will focus on gathering network metrics primarily using TrellisWare's MissionPlanner (MP) software for device, network, and RF link performance metrics as they pertain to voice-priority MANET communications.

   a. Controlled – static: The experiment will begin with establishing benchmark metrics for static nodes with known good RF and network quality of service. This test will be conducted at various distances ranging from 1-kilometer to 4 kilometers utilizing three configurations.

      i. Point-to-point column: this configuration will require the use of 5-12 personnel to spread out in a linear fashion at regular intervals from the CP out beyond the CP line of sight (LOS). Both the distant end and CP will have radios paired with agent radios to collect network and RF data via the MP software. Each radio will perform as a relay between the CP and end point radio. Voice test will be sustained for at least 5 minutes to gather enough data.

      ii. Cluster: this configuration will require three teams of radios. A team of 2 radios will be in the vicinity of the CP, the second team will be a cluster of 5-10 radios within LOS distance, and the third team will be 2 radios beyond team two's LOS. Voice traffic will be passed from team 1 to team 3, using the cluster of team 2 radios for relay. Voice test will be sustained for at least 5 minutes to gather enough data.

      iii. Point-to-point: this configuration will require 6 radios. There will be 3 pairs of radios all within LOS distance of each other, but each pair set for a different voice channel. There will be agent radios set to poll data. Voice test will be sustained for at least 5 minutes to gather enough data.

   b. Controlled – dynamic: This will use the same configurations, but will require units to be moving.

      i. Point-to-point column: same SoM as static, but dispersion between each node will increase until voice traffic is no longer tenable. At which point, dispersion will contract until voice traffic between the CP and end node is reestablished. Voice test will be sustained for at least 5 minutes to gather enough data.

ii. Cluster: both team 2 and 3 will move from the CP until voice traffic is no longer established. Team 2 will decrease themselves and the CP until voice is reestablished. Team 3 will then disperse from team 2 until voice traffic is no longer established and then move back towards team 2 until voice is reestablished with CP. Voice test will be sustained for at least 5 minutes to gather enough data

iii. Point-to-point: same SoM as static, but each pair will increase dispersion until voice is lost, and then contract distance until voice is reestablished. Voice test will be sustained for at least 5 minutes to gather enough data.

b. **Data Mesh Experiment:** Same SoM as voice-priority experiment, but sending text and video from the pause, at regular distance intervals, instead of voice only traffic.

c. Mix **Data/Voice Mesh Experiment:** Same SoM as voice-priority experiment, but including both text and video traffic from the pause, at regular distance intervals.

4. Logistics

a. TrelisWare TW-230 Requirements

(20) TW-230 Radios

(2) Laptop loaded with TW Mission Planner support software

(14) Foot Patrol Personnel

(25) Lithium Batteries (MBITR or similar)

(5) TW-230 Ethernet Adapters

(20) Radio Handsets

5. Execution Matrix

	17 MAY 2012	18 MAY 2012
0800-1100	Set-up and Operational Checks	Mesh Voice/Data network series
1100-1400	Mesh voice network series	Tear-Down
1400-1700	Mesh data network series	Secure Equipment and Hot Wash
1800-2000	Working Dinner	Travel

APPENDIX B. WAVE RELAY™ QUAD RADIO ROUTER AND MANET DATA LINK DATA SHEETS

PERSISTENT SYSTEMS

Quad Radio Router (WR-RTR2)

The **Quad Radio Router** offers deployment flexibility, robust fault tolerance, and unmatched scalability for large MANET systems, all in a compact and rugged package It contains up to four separate wireless radios, all of which participate in the routing.

The Quad Radio Router includes five 10/100 Mbps Ethernet ports that are IP67 rated and designed for outdoor use. An integrated NATO Audio 6-pin U-283/U connector enables standard push-to-talk headsets and speaker boxes to be connected to the system. Two RS-232 serial ports are available that enable serial-over-Ethernet connectivity.

The Quad Radio Router can be vehicle mounted for mobile deployments, mast mounted to cover large geographic areas, and/or paired with a Tracking Antenna System Kit to provide long-range, air-to-ground connectivity.

- Unmanned Systems
- Marine Deployments
- Tactical Networks
- Vehicular Networks
- Tracking Antenna System
- Sector Antenna Array

SITUATIONAL AWARENESS. FOR EVERY SITUATION.

VIDEO DATA VOICE

FIPS VALIDATED 140-2

MADE IN USA

GSA Schedule Contract

Contract # GS-35F-0168Y

Small Business

Persistent Systems, LLC | 303 Fifth Avenue, Suite 306 | New York, NY 10016 | O 212-561-5895 | F 212-202-3625 PersistentSystems.com

Security

- Integrated hardware cryptographic accelerator
- FIPS 140-2 Level 2 (Validated by NIST)
- Utilizes all Suite B algorithms
- 256-bit AES Encryption with SHA-512 MAC on Backbone
- Transport Layer Security (TLS) to Web Management Interface
- Active response to tamper
- Key Zero while Powered Off

Management

- Web Management Interface
  - Network Wide Firmware Upgrade
  - Network Wide Management/ Configuration Functionality
- SNMP Monitoring
- Google Earth Based Network Monitoring

Networking Capability

- Hybrid Routing Protocol Optimized for Mobility
- Throughput Optimized Routing Metric
- Maintains Connectivity under Mobility
- True Peer-to-Peer Connectivity
- No inherent scalability limit
- Seamless Layer 2 Integration - Routed Switching Architecture
- Optimized for Real-time Traffic (Voice/Video)
- Optimized for Multicast Traffic
- Optional 802.11 b/g Access Point

SITUATIONAL AWARENESS

- Simple Integration with Google Earth
- Cursor-on-Target Support (CoT) Proprietary DOD SA Message Support*
- Integration with FalconView*

*Available only to government customers

Native Voice Capability

- Supports up to 16 channels of Push-to-talk (PTT) Voice
- Operates in single or multi-channel mode
- G.711 Codec for Radio-over-IP (RoIP) interoperability
- Integrates with advanced PTT devices

Manufacturing & Warranty

- Designed and manufactured in USA
- Limited one year warranty
- Sustainment programs available
- Training facility available
- Training led by industry-leading experts

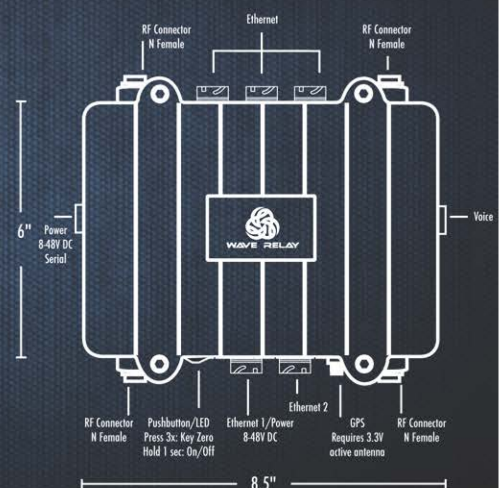
QUAD RADIO ROUTER SPECIFICATION SHEET

Specifications

Number of Radios	4
Peak TX Power	2 W*
Channel Access	CSMA/CA
Modulations	OFDM with Adaptive Modulation Algorithms
Channel Width	5, 10, 20 or 40 MHz
Throughput	37 Mbps UDP (20 MHz channel) 27 Mbps TCP (20 MHz channel)
Antenna Ports	4 N-Type Female RF Ports
Size	8.5 x 6 x 2 inches
Weight	3.2 lbs
Enclosure	IP67 Submersible Outdoor Rated
Ethernet Ports	IP67 10/100 Mbps with Auto MDI Port 1 – Power and Ethernet Port 2-5 – Ethernet only
GPS	Integrated GPS Receiver via SMA Female Connector
Voice	NATO Standard U-283/U Voice Connector
Mounting Options	Pole, Wall, or Magnetic Mount

*2 W version available only to military customers

Frequency Options	
Standard	**Optional**
S-Band 2.3 – 2.5 GHz 600 mW or C-Band 5 GHz	700 MHz, 900 MHz, 2.3 - 2.5 GHz, 2 W, 3 GHz, 4.9 GHz



Environmental

Operating Temperature	-40 to 85°C
Cooling	Convection Cooled without fans

Power

Power Consumption	<16W
Power Supply	8 - 48 VDC via PoE on Port 1 8 - 48 VDC via 4-Pin Port


PERSISTENT SYSTEMS
Wave Relay™ MANET Datalink
The Wave Relay™ MANET Datalink was designed as a small, lightweight embedded module ideal for integration with UAV/UAS, Robotics, Portable Ground Controllers, and other integrated systems. Seamless Layer-2 Ethernet connectivity facilitates plug-and-play operation of cameras, video encoders, IP sensors, and other devices. Serial to Ethernet functionality enables control of serial devices over the wireless network. The Flex Board design allows the integrator to access all the capabilities of Wave Relay™ technology in a compact form factor.
Wave Relay™ is a Mobile Ad Hoc Networking system (MANET) designed to maintain connectivity on the move. Wave Relay™ is a scalable, true peer-to-peer topology providing data, serial, and voice for demanding customer requirements. With user throughput of 37Mbps UDP and 27 Mbps TCP Wave Relay™ provides a dynamic, reliable, and secure wireless networking solution beyond mesh.
Wave Relay 2.3 to 2.5 GHz 2W Radio v4
▪ Peer-to-Peer MANET
▪ Seamless Layer-2 Ethernet Connectivity
▪ Supports Multicast Voice & Video
▪ Serial to Ethernet Capability
▪ Compact, Lightweight Design
▪ Tested to 100 Miles
▪ Up to 2 W Transmit Power*
FIPS VALIDATED 140-2
GSA Schedule Contract
Contract # GS-35F-0168Y
Small Business
*2 Watt module only available to military customers
MADE IN USA
Persistent Systems, LLC | 303 Fifth Avenue, Suite 207 | New York, NY 10016 | O 212-561-5895 | F 212-202-3625 PersistentSystems.com

Security

- Integrated hardware cryptographic accelerator
- FIPS 140-2 Level 1
- Utilizes all Suite B algorithms
- AES-CTR-256 with SHA-512 HMAC
- AP Encryption – WPA2-PSK

Management

- Secure Web Management interface
- Network wide firmware update
- Network wide management and configuration functionality
- Google Earth Based network monitoring

Networking

- Cursor-on-Target (CoT)
- Wave Relay Over IP (WRoIP)
- Industry leading Wave Relay™ MANET routing
- Seamless Layer 2 network connectivity
- IPV4
- Integrated DHCP client and server
- 802.11 a/b/g AP concurrent with MANET
- Integrated Serial-to-Ethernet capability
- Dynamic Link Exchange Protocol (DLEP) Certified

Native Voice Capability

- Supports up to 16 channels of Push-to-talk (PTT) Voice
- Operates in single or multi-channel mode
- G.711 Codec for Radio-over-IP (RoIP) interoperability
- Integrates with advanced PTT devices

Manufacturing & Warranty

- Designed and manufactured in USA
- Limited one year warranty
- Training facility available
- Courses led by industry-leading experts

WAVE RELAY MANET DATALINK SPECIFICATION SHEET

Specifications

Modulations	OFDM with Adaptive Modulation Algorithms
Channel Width	5, 10, 20 or 40 MHz
Throughput	37 Mbps UDP (20 MHz channel) 27 Mbps TCP
Radio	(1) MMCX Connection
GPS	(1) U.FL Connection
Size	2.685" x 3.890" [68.20mm x 98.80mm]
Thickness	.645" (16.4mm) with 2 Watt Card
Weight	3.25 oz / 92.1 g (with 2 Watt Radio)

Data Connection

20-Pin Flex Connector	10/100 Ethernet (2) RS-232 Serial PTT Audio 8 - 48 VDC Input Power 3.3 VDC Accessory Power

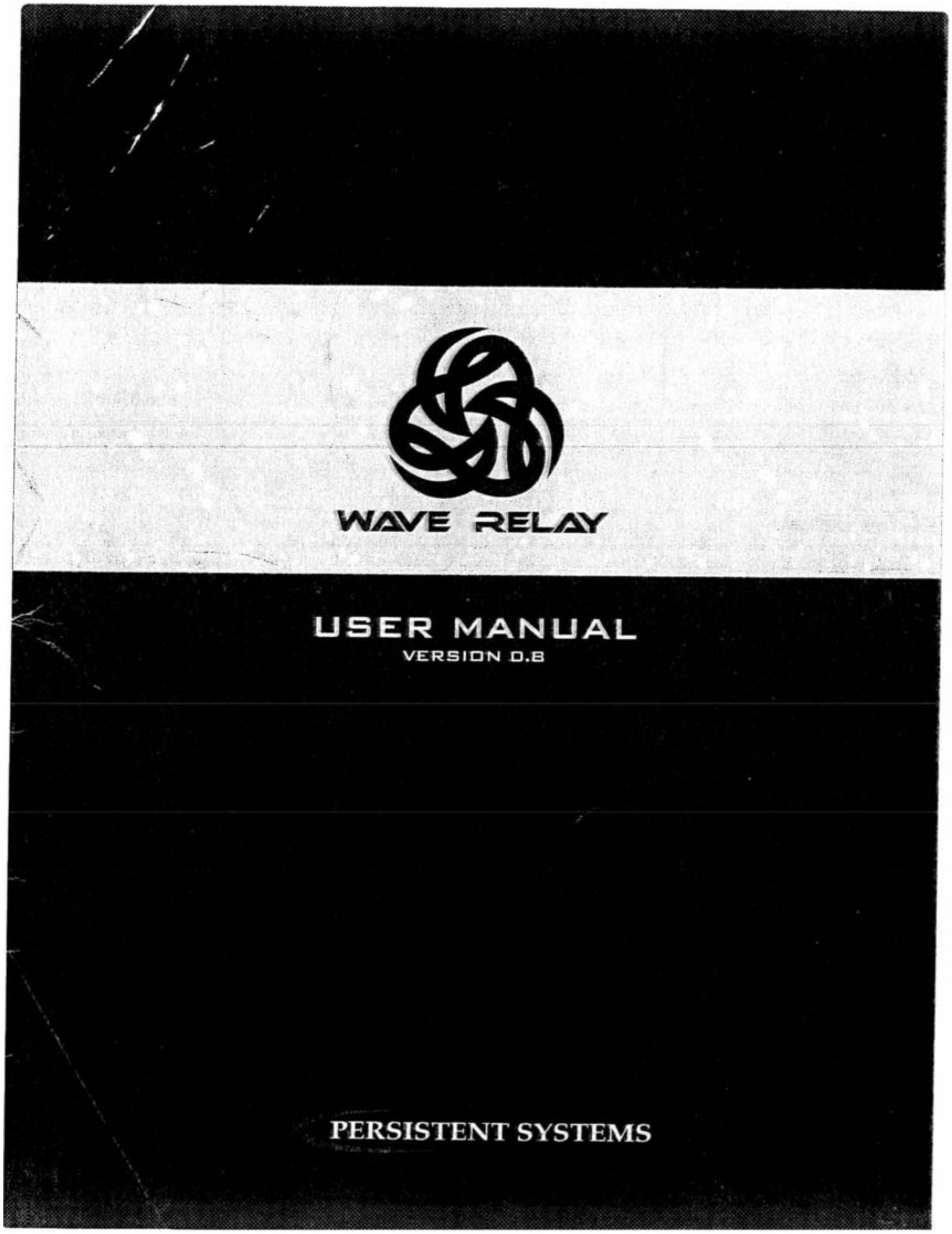
Power & Environmental

Power Consumption	Average - 4 W Peak - 18 W
Operating Temperature	-40° to 85°C

Available Frequencies

700 MHz
900 MHz
1.35-1.39 GHz (L-Band)
2.3-2.5 GHz (S-Band)
2.412-2.462 GHz (ISM Band)
4.4-5 GHz (C-Band)
4.9 GHz (Public Safety Band)
5.1-5.9 GHz
2.3-2.5 GHz 2 W High Power (S-Band)

APPENDIX C. WAVE RELAY™ USER MANUAL



INTRODUCTION

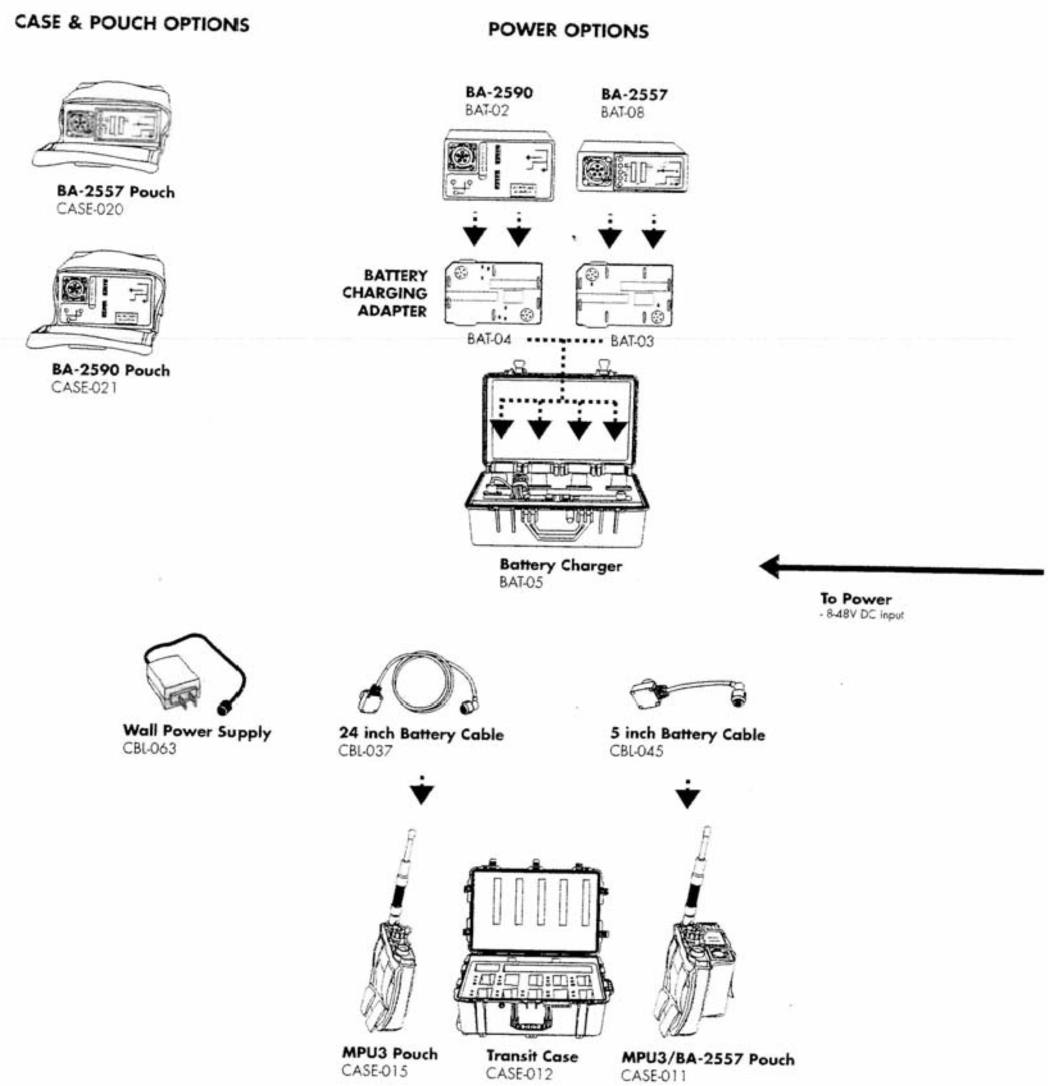
Wave Relay™ is a Mobile Ad Hoc Networking system (MANET) designed to maintain connectivity among devices that are on the move. The system is scalable, enabling it to incorporate vast numbers of meshed devices into the wireless network, where the devices themselves form the communication infrastructure. The result is a true peer-to-peer topology, unsurpassed fault tolerance, and high performance connectivity. Wave Relay™ provides a dynamic, reliable, and secure wireless networking solution for the military, public-safety first responders, and municipalities. Wave Relay™ offers all of these capabilities in an integrated and cost-effective package.

Wave Relay™ delivers an advanced mobile networking solution, beyond mesh. Even in highly dynamic environments, the system is able to maintain connectivity by rapidly re-routing data. Wave Relay™ does not merely "self-form" and "self-heal" as nodes move unpredictably throughout the network. Instead, high performance routing adapts quickly to fluctuations in terrain and other environmental conditions, continuously maximizing the communication performance.

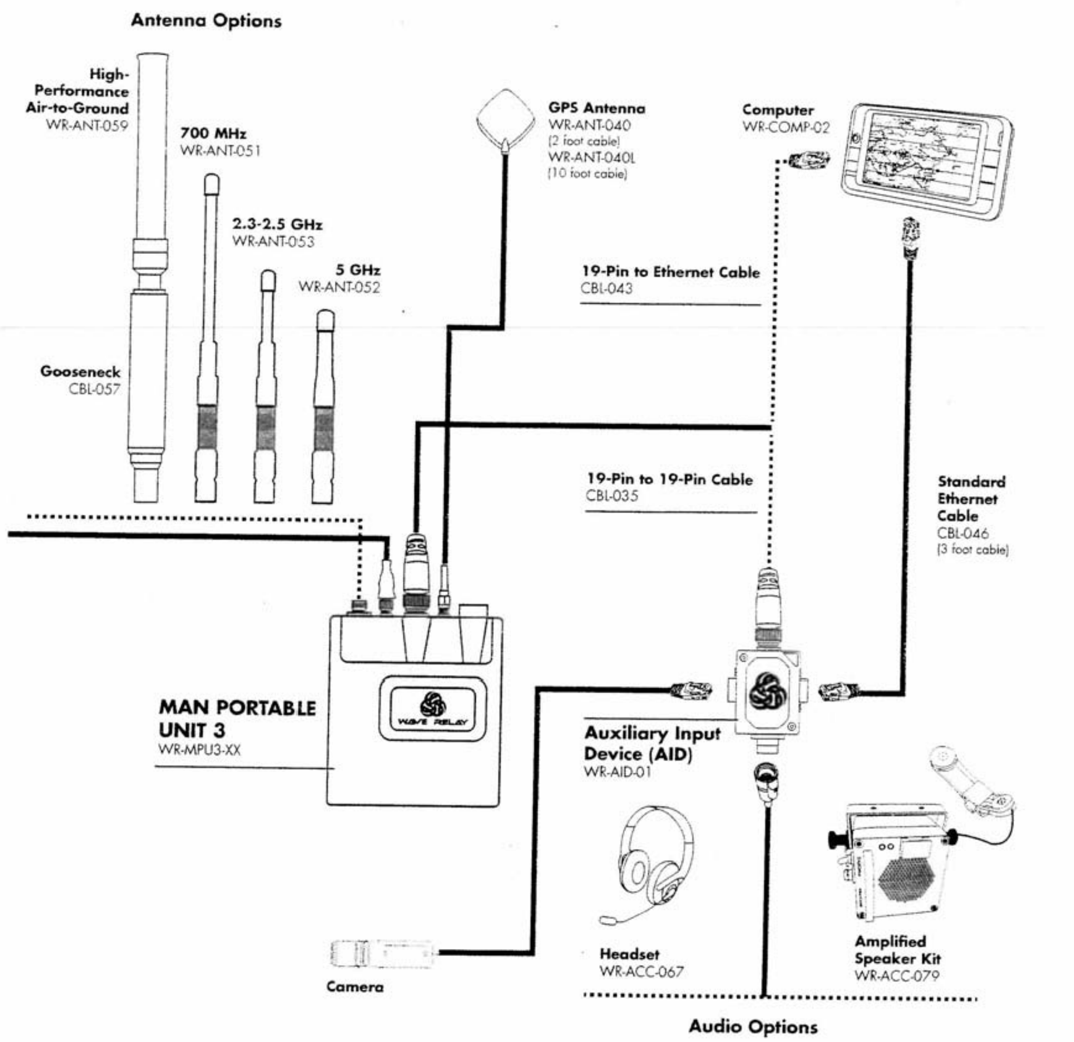
The Wave Relay™ System is a true peer-to-peer wireless mesh networking solution in which no device has special capabilities. If any device fails, the rest of the devices continue to communicate using any remaining connectivity. By eliminating master nodes, gateways, access points, and central coordinators from the design, Wave Relay™ delivers extremely high levels of fault tolerance regardless which nodes might fails.

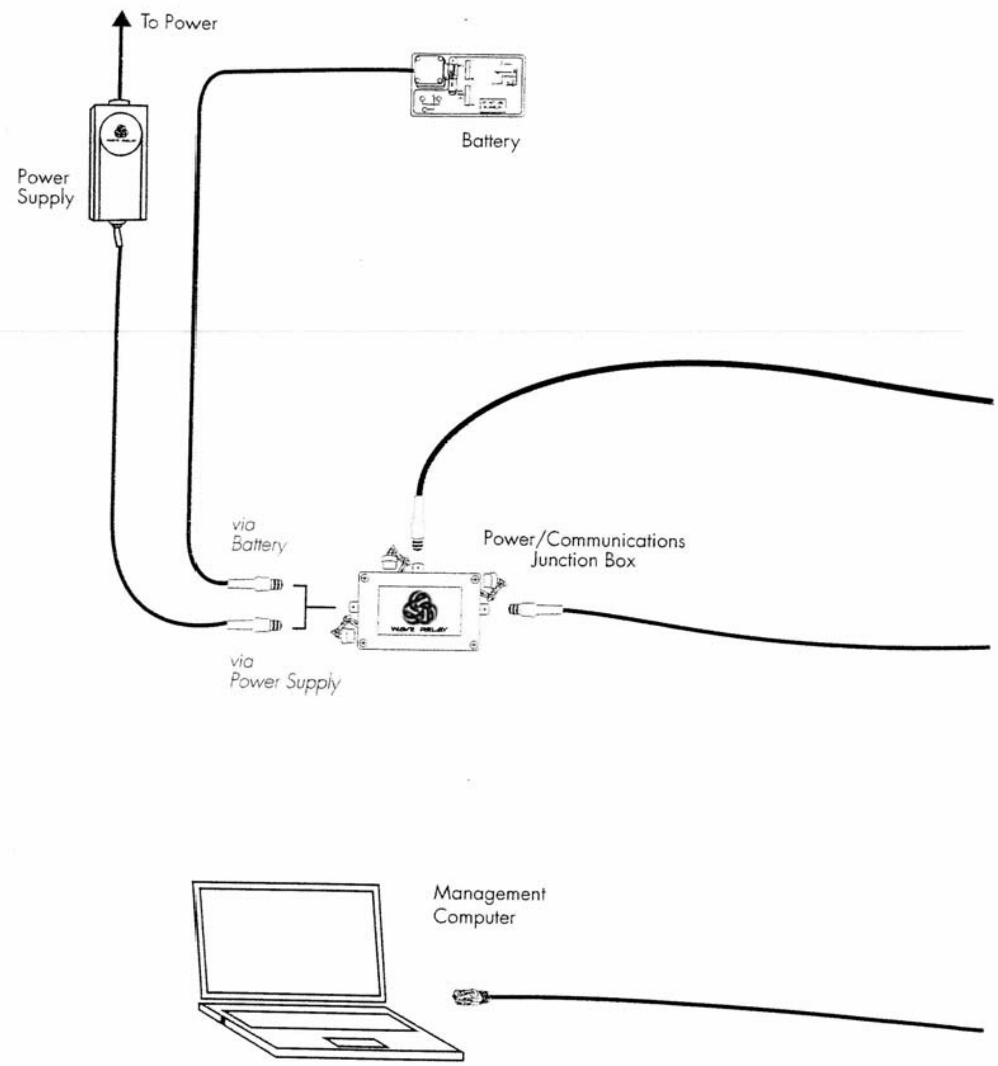
Military networks in particular rely heavily on multicast and broadcast communication to disseminate tactical information. The Wave Relay™ System is designed to maximize the broadcast capacity of the network and to minimize the overhead caused by such broadcast message dissemination. While optimizing efficiency, Wave Relay™ also implements techniques that increase broadcast reliability. The advanced multicast functionality allows the system to support both multicast voice and video over IP.

Due to Wave Relay's™ architecture, deploying the system and establishing the network are as easy as plugging in an Ethernet cable. The system operates on the data link layer (OSI Layer 2) rather than the network layer (Layer 3), facilitating plug-and-play operation. Indeed, Wave Relay™ is a truly seamless wireless Ethernet radio system offering dynamic and reliable solution for all networking needs.

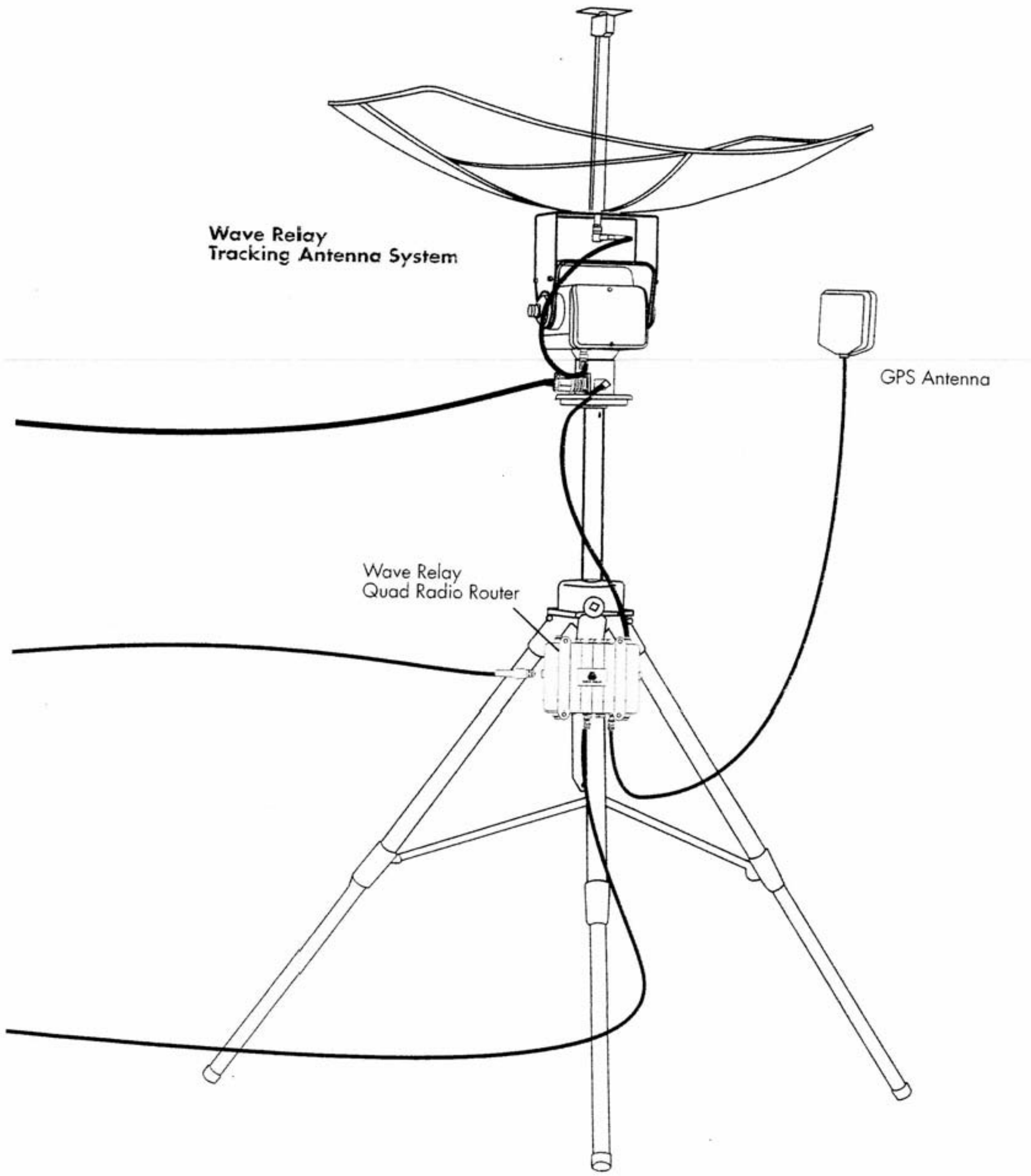

CASE & POUCH OPTIONS
POWER OPTIONS
BA-2557 Pouch
CASE-020
BA-2590 Pouch
CASE-021
BA-2590
BAT-02
BA-2557
BAT-08
BATTERY CHARGING ADAPTER
BAT-04
BAT-03
Battery Charger
BAT-05
To Power
- 8-48V DC input
Wall Power Supply
CBL-063
24 inch Battery Cable
CBL-037
5 inch Battery Cable
CBL-045
MPU3 Pouch
CASE-015
Transit Case
CASE-012
MPU3/BA-2557 Pouch
CASE-011

MAN PORTABLE UNIT (MPU3) KIT




To Power
Power
Supply
Battery
via
Battery
via
Power Supply
Power/Communications
Junction Box
Management
Computer

TRACKING ANTENNA SYSTEM KIT



This section of the manual discusses how to configure an individual device from factory settings. Follow this procedure for every device.

POWER THE DEVICE

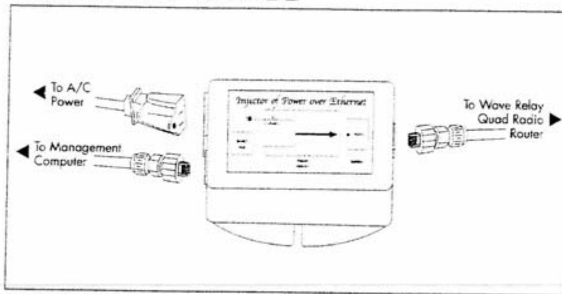


FIGURE 1: PoE injector configuration

Quad Radio Router

The Quad Radio Router can be powered either over Ethernet or via the integrated 4-Pin accessory port[1].

To power via PoE, use the supplied PoE injector and a standard Ethernet cable. Connect the output port on the PoE injector to the "Ethernet 1 Power" port on the unit. Connect the PoE injector to AC power (See Figure 1). The Ethernet port accepts 12 – 48 V DC. If the unit does not turn on immediately, press the pushbutton until the green LED illuminates.

To power via the integrated 4-Pin accessory port, insert the 4-Pin plug into the 4-Pin accessory port and twist the metal latch clockwise to secure the cable. The plug part number is Amphenol MS3116E8-4P. The 4-Pin accessory port accepts 12 – 48 V DC. Connect the other end of the cable to a DC power source or to an external battery pack (See Figure 2). Press the pushbutton until the green LED illuminates. If the unit does not turn on immediately, press the pushbutton until the green LED illuminates.

Man Portable Unit

The Man Portable Unit (MPU) can be powered over Ethernet[2], through the integrated 2-Pin accessory port, or with internal batteries.

To power via PoE, use a standard PoE injector and a standard Ethernet cable. Warning: Ensure that the device is PoE-capable before proceeding; only MPUs that have knurled battery caps feature PoE. Connect the output port on the PoE injector to the Ethernet port on the unit. Connect the PoE injector to AC power. The Ethernet port accepts 12 – 48 V DC. The unit will turn on though the LEDs will not illuminate.

To power via the integrated 2-Pin accessory port, use the supplied cable assembly[3]. The 2-Pin accessory port accepts 12 – 24 V DC. The mating connector is Tajimi R05-PB2M, where Pin-A is power and Pin-B is ground (see "Pin Out" (pg. 20)). Insert the plug and twist the metal latch clockwise to lock the cable in place. Press the pushbutton for one second, and the green LED will illuminate. Note that the red LED may illuminate as well.

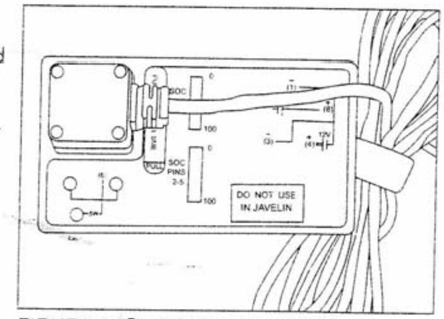


FIGURE 2: Proper battery cable orientation

To power via internal batteries, insert 12 AA Energizer Ultimate/Advanced Lithium batteries into the battery tubes. Insert the postive (+) end of the battery first. Press the pushbutton for one second, and the green LED will illuminate. The red LED indicates low internal batteries.

[1] Older models of the Quad Radio Router do not feature a 4-Pin port.
[2] Only MPUs that have knurled battery caps feature PoE.
[3] The MPU A/C adapter is available as an optional accessory.

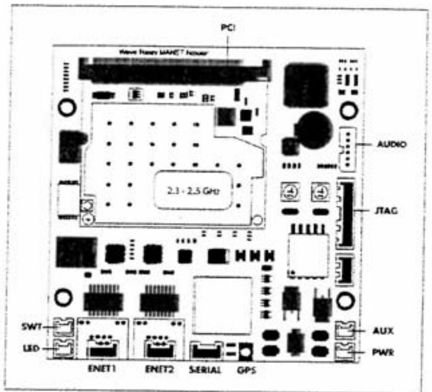


FIGURE 3: Single Radio Board Diagram

OEM Board

To power via PoE, use the Starter Cable Set with a 2-Pin connector, 4-Pin connector, and an RJ45 connector. Connect the 2-Pin connector to PWR, connect the 4-Pin connector to ENET1 or ENET2, and connect the RJ45 to the PoE device (see Figure 3). The board accepts 8-48 V DC.

To power via an external power supply, use the Starter Cable Set with only a 2-Pin connector. Connect the 2-Pin connector to PWR, and connect the bare wires to an external power supply. Then use the Starter Cable Set with only a 4-Pin connector to connect a computing device to ENET1 or ENET2. There are two cables with only 4-Pin connectors, enabling connection to both ENET1 and ENET2.

CONNECT TO THE WEB MANAGEMENT INTERFACE

Turn on the unit and connect it to the management computer with a standard Ethernet cable. If powering via PoE, connect the Ethernet cable to the "Data Input" port on the PoE injector (See Figure 1).

The management computer must be configured to be in the same IP Subnet as the unit. A permanent factory setting for the unit IP address is 10.3.1.254[1]. Configure the management computer as follows:

IP Address	**10.3.1.10**
Netmask	**255.255.255.0**
Gateway	**10.3.1.1**

Open a web browser on the management computer and connect to http://10.3.1.254. Each time you connect a new device, you may need to accept a security certificate before you can enter the Web Management Interface. The default password is "password", which should be entered in the dialogue box. Login.

A unit can always be accessed using this IP address so long as the management computer is configured as above and only one device is connected. However, since network operations require nodes to have unique IP Addresses, it is necessary to assign a new IP address (see "Assign a New IP Address" (pg. 5)) and to reconfigure the management computer to be in the same IP Subnet.

QUICK CONFIGURATION

If the network administrator provides a node configuration file, use it to facilitate quick device configuration. Please refer to "Quick Setup" (pg. 13). If a node configuration file has not been provided, follow the steps below.

ASSIGN A NEW IP ADDRESS

Whereas the permanent factory IP Address cannot be changed, the management IP Address can be changed. To change the management IP Address, connect to the Web Management Interface. Go to "Node Configuration - Node Configuration." Insert the new IP Address in the indicated field (see Figure 4). Per standard IP networking, the

[1] This is true for Ethernet 1 on the Quad Radio Router, Man Portable Unit, and OEM Board. The permanent, factory setting IP address for Ethernet 2 on the Quad Radio Router is 10.3.2.254.

change on computer too.

new IP Address and the Gateway must be in the same Subnet. To change the Gateway, uncheck "Use Network Default", and specify a Gateway in the same Subnet as the new IP Address. Scroll to the bottom of the page and select "Save & Reconfigure Unit."

The Web Management Interface can now be accessed using the new IP Address so long as the management computer and the unit are in the same subnet. The purpose of assigning a new IP address is to facilitate node management. In addition, you only need to accept the security certificate once.

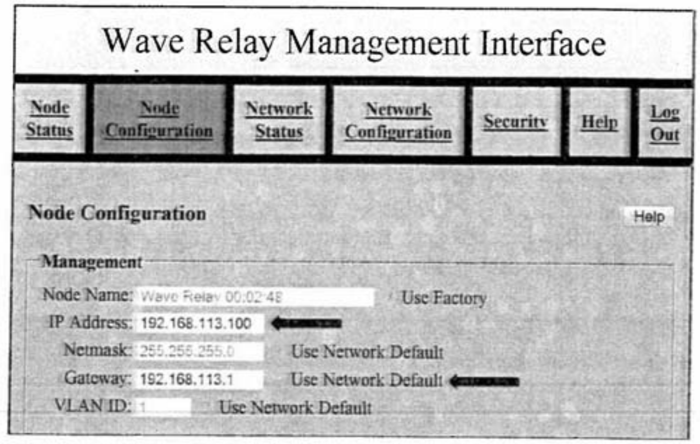


FIGURE 4: The IP Address and the Gateway are in the same Subnet.

CHANGE THE NODE NAME

The Node Name can be changed from the same configuration screen. Go to "Node Configuration - Node Configuration." In the Node Name field, uncheck "Use Factory", and insert the new name in the appropriate field. Scroll to the bottom of the page and select "Save & Reconfigure Unit".

This section discusses Network Configuration, which affects all the nodes in a network.

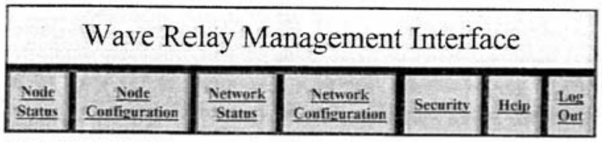


FIGURE 5: Web Management navigation bar

WAVE RELAY WEB MANAGEMENT INTERFACE

The Wave Relay Web Management Interface enables users to configure and to monitor Wave Relay units through a web browser. A navigation bar organizes the Management Interface. The linked pages outlined in red pertain only to the node to which the management computer is connected (either by Ethernet cable or by wireless), and the linked pages outlined in blue pertain to the entire network of nodes (see Figure 5). The logic behind Wave Relay management is that users configure network settings once and then configure individual nodes to use those network settings. Rather than to change individual node settings, users need only change network settings that then propagate to all nodes defined in the Node List.

MANAGE NODE LIST

Access "Manage Node List" under "Network Configuration" from the navigation bar. The Management Interface allows routers to be managed individually or as a network. To manage routers as a network, the Node List must be configured. The Node List contains a list of nodes specified by IP Address that are controlled by the Management Interface. Any function that resides under Network Status or Network Configuration operates on, and only on, the nodes listed in the Node List. The Node List does not limit connectivity between nodes. Two nodes are able to communicate even if they are not in the same Node List. However, network functions can only be applied to nodes in the Node List.

NETWORK -VS- MANAGED NODES DEFINED

In the context of Wave Relay, the network is defined as the set of nodes for which routing is possible. These nodes do not need to be specified in the Node List. By contrast, the Node List defines a set of nodes that are managed by the Web Management Interface. That list, however, does not restrict routing between nodes specified in the Node List and nodes not specified in the list. Therefore, the Node List is just a management tool that defines the list of nodes on which management functions operate. In general, the Node List should be updated whenever the network changes in order to ensure that every node contains complete and current information and is able to be monitored and controlled by the Web Management Interface[1].

CONFIGURE DEFAULTS

Network Defaults facilitate the management of a large number of nodes. The Network Defaults enable administrators to manage settings on all network nodes specified in the Node List rather than to manage individual settings on single nodes. To ensure proper Network Default configuration, confirm that the Node List is current and configured properly before making changes to Network Defaults. Any changes to Network Defaults will only affect nodes that are in your Node List. To access Network Defaults, go to "Network Configuration - Manage Node List."

Network Default settings are distributed to all nodes in the Node List. However, individual nodes do not necessarily use those settings. Only those individual nodes set to use the Network Default will use the settings specified in Network Defaults. See Individual Node Configuration (pg. 10).

Reconfigure the Network and Require All

Once Network Defaults are configured, save them to the network by selecting "Save to Network" at the bottom of the page. (see Figure 6). There are two check boxes at the bottom of the page.

[1] If the Node List is changed but the network is not updated, the new Node List is saved only to a local file. While not standard operating procedure, such an operation can be useful to manage a subset of nodes on the network.

When "Reconfigure the Network" is checked, saving applies the Network Defaults and reboots all devices in the Node List. This operation causes up to a minute of network downtime. During mission critical operations that cannot tolerate such disruptions, ensure that the box is not checked. The Network Defaults will be distributed to all devices in the Node List but not applied. During scheduled maintenance or other appropriate times, the Network Settings can be applied by checking the box and saving.

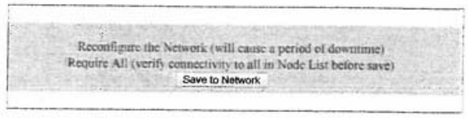


FIGURE 6: "Node Configuration" saving options

The "Require All" check box verifies connectivity to all devices in the Node List before Network Defaults are saved. When checked, this option ensures that all devices in the Node List have the same Network Defaults; the Network Defaults are not saved if connectivity to any devices fails. When unchecked, this option saves the Network Defaults to only those devices in the Node List for which connectivity is available. This option is useful when there are many devices in the Node List, some of which may be powered off or otherwise unreachable.

NETWORK UPGRADE

Network Upgrade installs new firmware versions on large numbers of nodes with one operation. Since network upgrades function on all nodes in the Node List, make sure the Node List is complete and current before performing a Network Upgrade.

Go to "Network Configuration - Network Upgrade." Browse to select the appropriate upgrade file. Check or uncheck "Require All." If checked, the update will be installed if and only if all the nodes in the Node List are accessible. If unchecked, the update will be installed to only those nodes in the Node List that are accessible. Network Upgrades will cause nodes to be reconfigured, an operation that causes a period of downtime. Do not perform Network Upgrades during mission critical operations that cannot tolerate such disruptions. Under such situations, perform Network Upgrades only during scheduled maintenance or other appropriate times.

Do not unnecessarily disturb devices during a Network Upgrade. Loss of power during the Network Upgrade can permanently damage a device.

CHANGE PASSWORD

The default management password is "password". This password is used to access the Web Management Interface. To change the management password, follow the directions under "Network Configuration – Change Password".

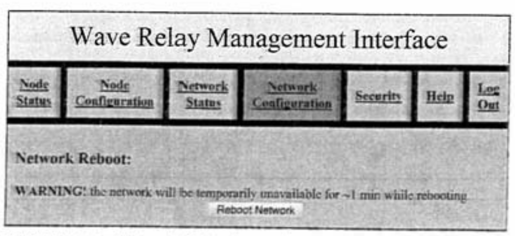


FIGURE 7: Network Reboot warning

REBOOT NETWORK

A Network Reboot functions on all the nodes in the Node List. To reboot a network, go to "Network Configuration - Network Reboot." Do not perform Network Reboots during mission critical operations that cannot tolerate interruption. Perform Network Reboots only during scheduled maintenance periods or other appropriate times.

One useful function of Network Reboot is to reboot a large number of nodes not physically accessible.

Rebooting causes a period of downtime. Do not perform Network Reboots during mission critical operations that cannot tolerate such disruptions.

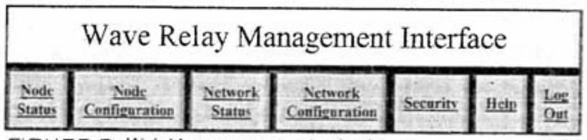


FIGURE 8: Web Management navigation bar

FIGURE 9: Radio 1 Enabled

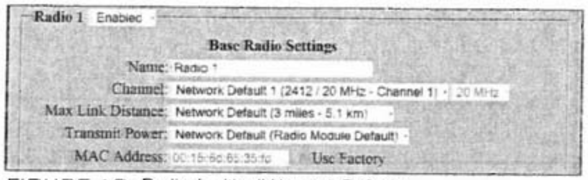


FIGURE 10: Radio 1 with all Network Defaults

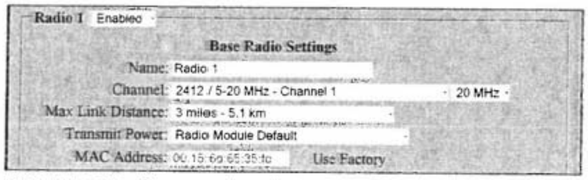


FIGURE 11: Same as above but none are Network Defaults

This section focuses on Node Configuration, which is on the "red" portion of the Web Management Interface (see Figure 8).

NODE CONFIGURATION

To access Node Configuration, go to "Node Configuration – Node Configuration."

The Node Configuration page is organized into categories (e.g. Radio 1). To view and to set the configuration settings, ensure that the category is "Enabled" (see Figure 9). Otherwise, the configuration settings are hidden. This is true not only for the entire Radio category, but also within the Radio category. For example, if the Access Point is disabled, then Access Point configuration settings are not viewable.

The page that follows presents node-specific settings. These settings include identifiers (e.g. IP Address), radio settings (e.g. channel), and GPS settings. Changes made to Node Configuration affect only one node, not the entire network of nodes defined by the Node List.

Consider the Radio 1 Configuration (see Figure 10). Here, Radio 1 on this node is set to operate on "Network Default 1 (2412 / 20 MHz – Channel 1)". The Radio 1 channel for this node only will adopt the channel setting specified in Network Defaults under Network Default 1, which is 2412 / 20 MHz – Channel 1. If Network Default 1 changes, then the setting for Radio 1 Channel changes with it.

Now, consider the next configuration (see Figure 11). Here, Radio 1 on this node is set to operate on "2412 / 20 MHz – Channel 1". This is not a Network Default channel, so the channel will remain unchanged if and when the Network Defaults are changed.

Even though Network Default settings are written to all nodes in the Node List, only nodes set to operate on those defaults will assume the Network Default settings.The same logic applies to all settings in Node Configuration.

Once all Node Configuration settings are complete, scroll to the bottom of the page and select "Save & Reconfigure Unit". This operation saves the settings and reboots the node. Do not perform this operation during mission critical operations that cannot tolerate interruption to the individual node. Perform it only during scheduled maintenance periods or other appropriate times. The Web Management Interface does not offer strict warning about this operation as it does with other Network-wide operations.

TRACKING CONFIGURATION

For assistance setting up the tracker, refer to the seperate Tracker Manual.

Access the Web Management Interface. Ensure the Node List is complete and current. In particular, ensure the node to be tracked is correctly specified in the Node List.

The Tracking Antenna System relies on GPS information from both the tracker and the tracked node. On both the tracker and the tracker node, ensure that "Position Settings" Update Interval is set to 1 sec and that "Google Earth Network Visualization Settings" Report to Visualization Server is set to Enabled. These setting are available at "Network Configuration - Configure Network Defaults".

Lastly, go to "Node Configuration - Tracking Configuration." Set "Tracking Antenna Control" to Enabled. Under "Tracking Antenna Mode," select the method to be used to track the node.

Track Node

Select "Track Node" or "Track Node w/ Initial Coordinates." Select the node is to be tracked. Enter the Compass Reading (further information available in the seperate tracker manual). If you selected "Track Node w/ Initial Coordinates," input the initial coordinates in addition to the previously mentioned fields. This is useful if the tracker loses connectivity with a node on a plane. A rendezvous point can be decided upon between the pilot and the node operator. The pilot will fly to the rendezvous point and the operator will set the rendezvous point as the initial coordinates on the tracker.

Track via External Feed

"Track via ESD Feed" and "Track via CoT Feed" both require a continuous UDP stream of ESD or CoT messages. These messages specifically tell the tracking system where the plane is located. In this mode, the tracking system will point at the location specified by the external feed, regardless of connectivity to the tracked node. Input the port on which the node will recieve the tracker information, then enter the Compass Reading.

If the tracked node is not powered on or does not have a GPS lock, then the antenna will not move. The tracker will be waiting to hear a GPS update from that node. Also, the tracker will not move until it knows its own position (e.g. its GPS locks or it is set to a manual position). Once the tracker knows where it is and hears GPS coordinates from the tracked node, the tracker will begin to track.

A Fine Tuning section is available if you need to fine tune the tracker. One way to do this is have the plane fly across the horizon and watch the tracker move with the plane. If you can visually see the that the tracker is off by a bit, you can manually adjust the fine tuning options so that the tracker lines up with the plane. Alternatively, you can adjust the fine tuning options and check to see if the SNR increases.

NODE UPGRADE

Perform a Node Upgrade when a new firmware version is available and there is only one device to upgrade. Whenever possible, use Network Upgrade instead of Node Upgrade to ensure that all devices in the Node List run the same firmware version. If a Network Upgrade is not possible, either because there is only one device to upgrade or other devices are inaccessible, be certain to upgrade other devices as soon as possible, since different firmware versions are not necessarily compatible. Warning: Never install an older firmware verison.

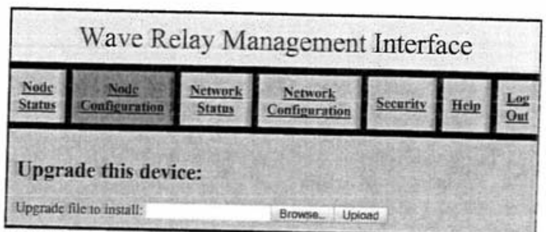


FIGURE 12: Node Upgrade

Go to "Node Configuration - Node Upgrade" (see Figure 12). Browse to select the appropriate upgrade file. A Node Upgrade will cause the node to be reconfigured, an operation that causes a period of downtime. Do not perform Node Upgrades during mission critical operations that cannot tolerate such disruptions. Under such situations, perform Node Upgrades only during scheduled maintenance or other appropriate times.

Do not unnecessarily disturb a device during a Node Upgrade. Loss of power during the Node Upgrade can permanently damage a device.

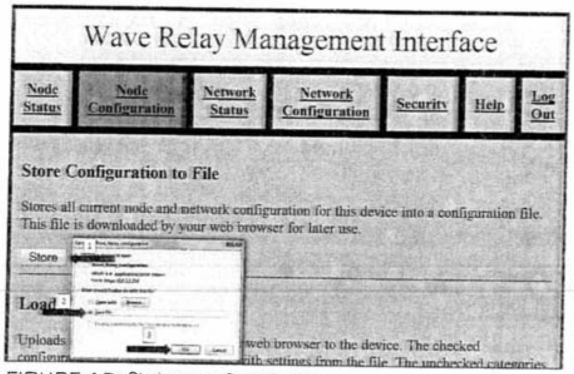


FIGURE 13: Storing a configuration file

CONFIGURATION MANAGEMENT

Device settings, both Node Configuration and Network Configuration, are stored to a local device file. This configuration file can also be stored elsewhere for later use. The configuration file provides both a backup for device settings and the ability to easily transfer settings from one device to another.

Store Configuration to File

Ensure Network Configuration and Node Configuration settings are as desired. Select "Node Configuration" from the navigation bar, and select "Configuration Mgmt" from the list. Clicking "Store" opens a prompt to choose where to save the configuration file. Note specifically that this file contains settings, both Network Configuration and Node Configuration, for only the current device (see Figure 13).

Load Configuration from File

To restore all settings back to a device, or to upload settings from another device, use the Configuration Management.

Select "Node Configuration" from the navigation bar, and select "Configuration Mgmt" from the list. Scroll down to the Load Configuration section. Click "Browse" and select the configuration file to be loaded. Note that the configuration file should be from a device with the same firmware version and hardware setup (e.g. numbers and types of radios) as the device to which it is being uploaded. All the settings from the configuration file need not be uploaded to the device. To select the configuration settings to be uploaded from the file to the device, check the appropriate configuration categories. The checked configuration categories on the device are replaced with settings from the file. The unchecked configuration categories on the device remain unchanged. Click "Load" to complete the setup (see Figure 14).

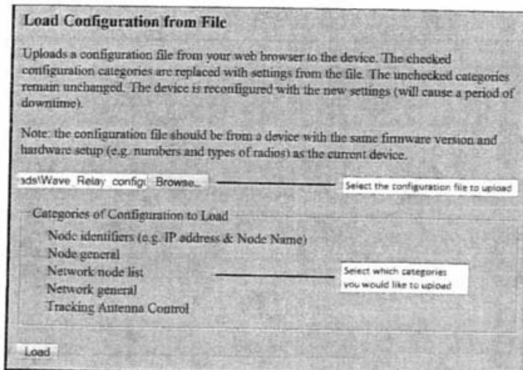


FIGURE 14: Loading a configuration file

QUICK SETUP

Both "Load Configuration from File" and "Quick Setup" load configuration settings from a configuration file. The difference between the functions is that "Quick Setup" loads all the configuration settings from a file (except Node Identifiers) whereas "Load Configuration from File" loads user-selected configuration categories. Quick Setup facilitates the configuration of a large number of nodes when the nodes share

identical configuration settings. Note specifically that the only configuration categories that must be specified when using Quick Setup are Node Identifiers, which include IP Address, Node Name, and SSPG SA ID.

Select "Node Configuration" from the navigation bar, and select "Quick Setup" from the list. Click "Choose File" and select the configuration file to load to the device. Note that the configuration file should be from a device with the same firmware version and hardware setup (e.g. numbers and types of radios) as the device to which it is being uploaded. Insert the IP Address, Node Name, and SSPG SA ID to be set to the device. Select "Setup". All settings from the configuration file will be applied to the device except IP Address,, Node Name, and SSPG SA ID, which will populate from the values specified (see Figure 15).

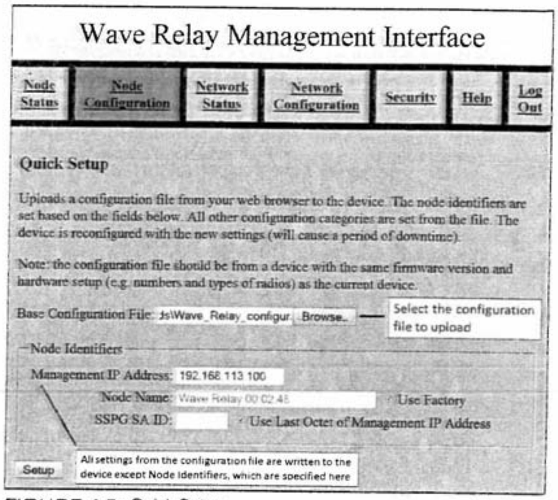


FIGURE 15: Quick Setup

REBOOT NODE

A Node Reboot power cycles an individual node. Do not perform Node Reboots during mission critical operations that cannot tolerate interruption to the individual node. Perform Node Reboots only during scheduled maintenance periods or other appropriate times. The Web Management Interface does not offer strict warning about Node Reboots as it does with Network Reboots.

One useful function of Node Reboots is to reboot a node not physically accessible.

ESTABLISH A NETWORK OF NEW NODES

This section describes an efficient method to establish a managed network. Ensure that all nodes are operating with the same firmware version.

USE QUICK SETUP TO CONFIGURE IDENTICAL NODES

Identical nodes are defined as nodes that have the same number of radios and hardware setup.

Access the Web Management Interface from one node. Setup the Network Configuration and Node Configuration (Note: A node cannot be configured properly if it is not keyed. If the "Security" tab on the Web Management Interface bar is blinking red, the node is not keyed. See "Security" section for more information on keying a device (pg. 20).) See "Initial device configuration" (pg. 4), "Network Configuration" (pg. 7), and "Individual Node Configuration" (pg. 10). Ensure that the Node List is populated with all of the node IP Addresses that will be in the final Network.

Store a configuration file. See "Store Configuration to File" (pg. 12).

Access individually every other identical node and use Quick Setup to load the configuration file. Enter a unique IP Address and Node Name for each node. The IP Addresses should match the ones in the Node List. Ensure that all IP Addresses are in the same Subnet.

Repeat this process for each set of identical nodes. For example, if there are two Quad Radio Routers and two Man Portable Units, then the Node List will have IP Addresses for all four nodes. First configure one of the two Quad Radio Routers. Save that Quad Radio Router configuration file and use Quick Setup to configure the other Quad Radio Router. Then setup one of the Man Portable Units, ensuring that its radio is set to the same channel as one of the radios on the Quad Radio Routers. Save that Man Portable Unit configuration file and use Quick Setup to configure the other Man Portable Unit.

SETTING A KEY

A node will not function properly if it does not have a security key. Make sure a valid security key has been set prior to configuring a node. If the "Security" tab on the Web Management Interface is blinking red, then a proper key has not been set.

Before nodes can communicate, they need to have the same key. Click on the "Security" tab on the Web Management Interface bar (see Figure 16). All nodes that are going to communicate need to have the same key AND the same Crypto Mode. If two nodes have the same key but different Crypto Modes, they will not be able to communicate. Once the Crypto Mode has been set, enter the security key you will use for all the nodes in the network. See "Security" (pg. 20) for further information on keys.

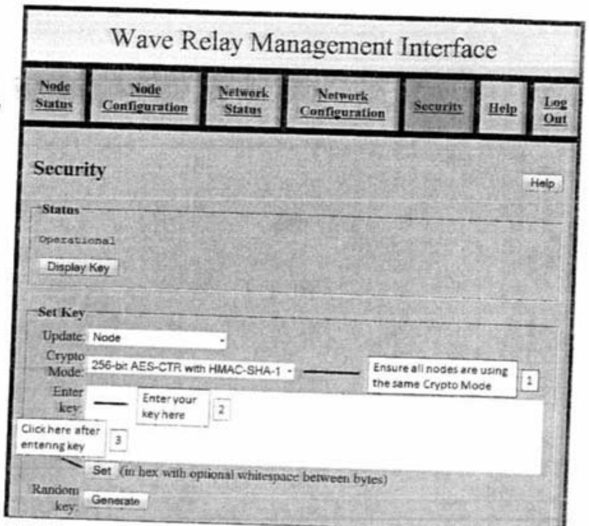


FIGURE 16: Setting up Security

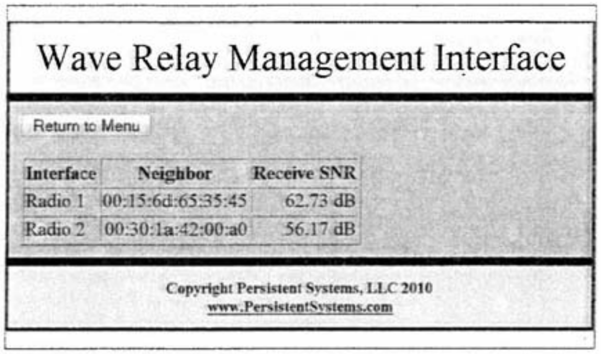


FIGURE 17: Neighbor SNR shows two neighbor radios

VERIFY CONNECTIVITY

Ensure that all nodes are turned on, that at least one radio on each node has an antenna and is set to the same channel as the other nodes, and that each node has the same key.

Access one of the nodes and verify connectivity to all the nodes. To do this, go to "Node Status - Neighbor SNR."

Figure 17 displays the Node Neighbor SNR. This shows which of the nodes radios are communicating with other radios. Figure 17 shows that radio 1 and radio 2 are each communicating with one other radio.

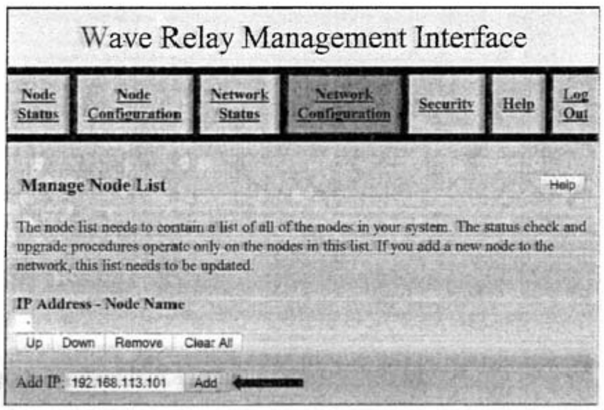


FIGURE 18: Adding a node to a Node List

ESTABLISH A NODE LIST

The Node List is a list of IP Addresses of nodes managed by the Web Management Interface. See "Manage Node List" (pg. 7). To manage the Node List, select "Network Configuration" from the navigation bar, and then select "Mange Node List."

On the following screen, add the IP Address of a node in the "Add IP" field and select "Add" (see Figure 18).

Repeat for every node to be managed. The IP Addresses will appear in the list. See Screen Shot. When the list is populated with all the IP Addresses, select "Update Network" (see Figure 19).

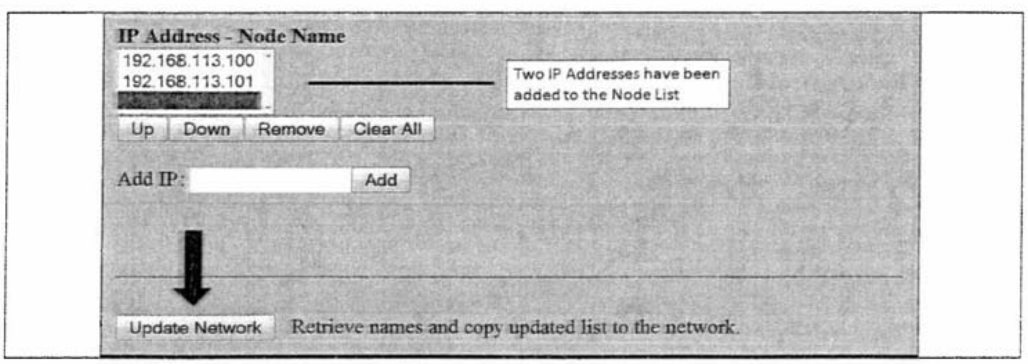


FIGURE 19: Updating a managed network with two nodes

When "Update Network" is selected, an attempt is made to contact every node specified in the Node List. If a node is available, its interface names are retrieved. If a node is not available, its old interface names are retained. A Master Node List, consisting of all the IP addresses specified in the Node List in addition to the names of all the interfaces, is created. The Master Node List is distributed to each available node in the Node List (see Figure 20).

If you go back to the Node Neighbor SNR, you will see a table in which the Node Names appear (see Figure 21). We now know that the two neighbors are two radios on the same node: "Wave Relay – 101."

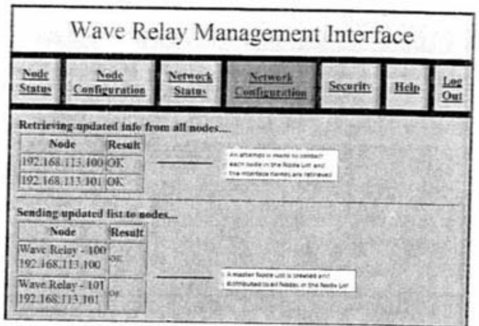


FIGURE 20: The nodes are successfully communicating

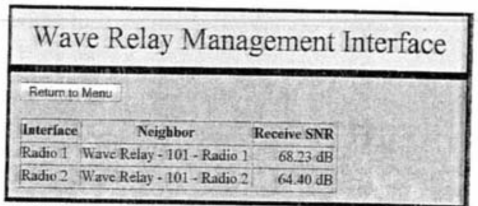


FIGURE 21: SNR with neighbor names displayed

ADD A NODE TO AN EXISTING NETWORK

This section describes how to add nodes to an existing network.

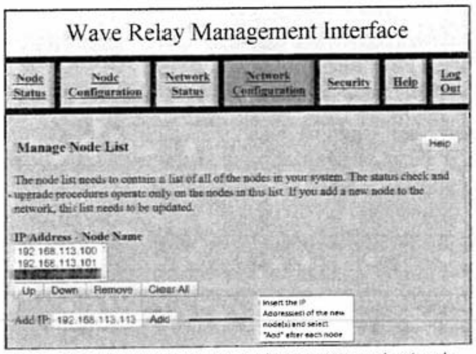


FIGURE 22: Adding a new node to a managed network

CONFIGURE INDIVIDUAL NODES

Verify connectivity to the new unit (see "Verify Connectivity" (pg. 15)).

If a configuration file was supplied, use that to get configure the new node (see "Use Quick Setup to Configure Identical Nodes" (pg. 14)).

Confirm that the new unit has a unique IP Address and Node Name. (See "Assign New IP Address" (pg. 5) and "Change the Node Name" (pg. 6)).

Confirm that the new Unit is on the same wired segment as the rest of the network or that it is configured to operate on the same channel as the other units in the network.

Through the Management Interface, access a unit on the network that is not the new Unit. If the new Unit is the only unit in the Network, then access the new Unit. Select "Network Configuration" on the navigation bar, and select "Manage Node List".

Add the new IP address in the box and select "Add" (see Figure 22). The new IP Address has been added to the Node List of the unit to which you are connected (see Figure 23). Note that the new node is added to the list above the position currently selected or, if no position is currently selected, at the end of the list. To add multiple units to the network, repeat the previous step for each new IP Address. In order to update the entire Network, select "Update Network" at the bottom of the screen. This function copies the updated Node List to the entire network, including the new unit(s)[1]. The Node List can be ordered in the same management area. The Node List order determines the order management functions are undertaken and reported.
For example, when Update Network is clicked, the new Node List will be distributed to all routers in the order in which they appear in the Node List.

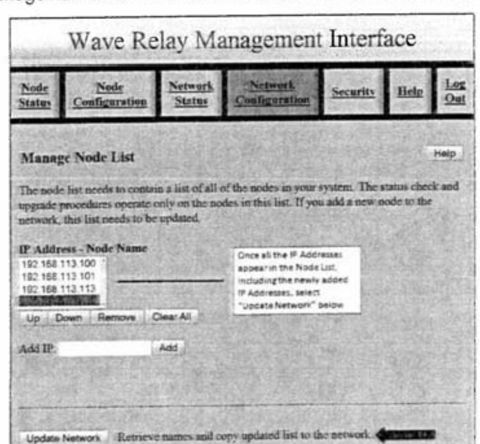


FIGURE 23: The new node has been added to the list

CONFIGURE NETWORK DEFAULTS

Make sure the new node has the same Network Defaults as the other nodes in the network. To do this, access a node in the network that is not the new node and go to "Network Configuration - Configure Defaults." Go to the bottom of the page and select "Save to Network." If the new node is the in Node List, the Network Defaults will get pushed to it.

[1] Pressing the "Update Network" button performs the following operations:

1. An attempt is made to contact each node in the Node List.
2. If a node is available, its interace names are retrieved. If a node is not available, its old interface names are retained.
3. A Master Node List, consisting of all the IP addresses specified in the Node List in addition to the names of all the interfaces, is created.
4. The Master Node List is distributed to each available node in the Node List.

LOG OUT

Logging out de-authenticates. After logging out, a management password is required to reauthenticate. Closing a browser window without logging out may allow a user to configure nodes without providing a management password. For network security purposes, it is important to log out after each session.

PUSHBUTTON

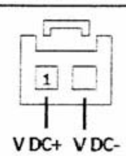
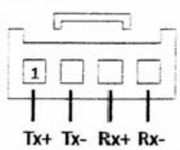
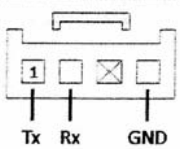
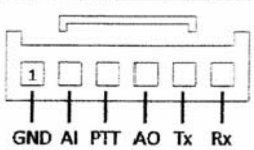
Quad Radio Routers and MPUs feature a multi-function pushbutton. Pressing and holding the button for a second will turn the node on or off. Pressing the button three times in quick succession will zero the security key.

Quad Radio Routers automatically remain in the "on" state so long as it is not turned off via the pushbutton before having power disrupted. In the same manner, a Quad Radio Router will stay off if it was turned off prior to having its power removed. This feature is useful if a node is mounted in a high place or otherwise unreachable location. As long as the unit is not turned off, there is no need to press the pushbutton when power is resupplied.

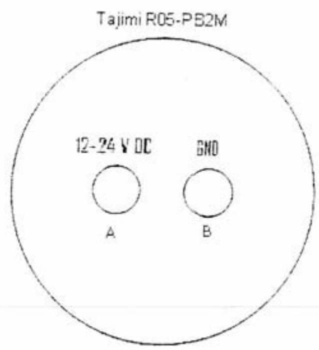
MPUs must always be turned on when power is disrupted.

CONNECTOR SPECIFICATIONS

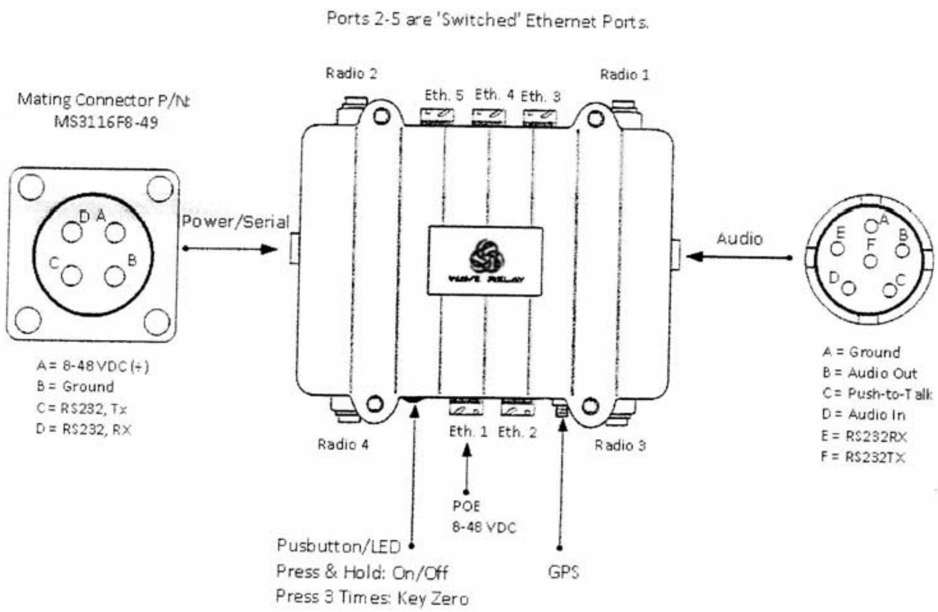
All mating connector parts available at Digikey.com

Connector	Pin Out	Mating Connector #
	**2 – Pin** **Power** **Aux Power**	**455-1486-ND**
	**4 – Pin** **Ethernet**	**455-1488-ND**
	**4 – Pin** **Serial**	**455-1488-ND**
	**6 – Pin** **Audio** **GND – Ground** **AI – Audio In** **PTT – Push-to-talk** **AO – Audio Out** **Tx – Wave Relay Tx to Device Rx (RS-232)** **Rx – Wave Relay Rx from Device Tx (RS-232)**	**455-1490-ND**

PIN OUT
MPU 2-Pin Power



Quad Radio Router



STATUS

The Status box indicates the current security configuration. "Operational" means a valid key is set and Wave Relay is operational. If Wave Relay is NOT operational, then the node will not communicate with any other nodes, and its management interface can only be accessed via connection to the Ethernet 1 interface. The Security tab on the navigation bar blinks red when the current status is not "Operational". If a node is booted without a key, "Error: no security configuration" will be displayed. In addition, an error will be displayed if the key has been zeroized.

The current key, if one is set, can be viewed by selecting "Display Key". Since the key is displayed in plaintext, view the key only in a secure environment. The "Display Key" feature indicates the current Crypto Mode, Size, and Value of the key.

SET KEY

The Set Key box enables users to change the current security configuration. Changes can be applied to the current node only or to all the nodes in the Network as specified by the Node List. Ensure all nodes are running the latest firmware before making changes to the security configuration.

To change the security configuration, choose whether to update the node or the entire network. Changes to the network may require all nodes to be accessible so that security configuration is fully distributed to all nodes in the Node List. In order to require all nodes in the Node List to receive new security configurations, select "Network - require all" from the update pull-down menu. Otherwise, select "Network - any available", a function that distributes new security configurations to only accessible nodes. If a changed key is distributed to only some of the nodes in the network, then those nodes will no longer communicate with nodes that did not receive the changed key.

The "Crypto Mode" sets the the encryption and authentication algorithms used to secure Wave Relay packets. The available set of crypto modes depends on the node's hardware capabilities. Newer Wave Relay products have extra hardware to support additional Suite-B algorithms (SHA-2 family and GCM) in comparison to older Wave Relay products, which do not.

Crypto Mode	256-bit AES-CTR with HMAC-SHA-512	256-bit AES-GCM	256-bit AES-CTR with HMAC-SHA-1
Availability	New Hardware Only		Both Old and New Hardware
Encryption Algorithm	256-bit AES in counter mode		
Authentication Algorithm	HMAC-SHA-512	Galois MAC (GMAC)	HMAC-SHA-1
MAC Tag Length	96-bits		
Suite-B Algorithms	Yes		No (due to SHA-1)
Minimum Key Length	512-bits (256-bit AES + 256-bit HMAC)	256-bits	512-bits (256-bit AES + 256-bit HMAC)
Maximum Key Length	1280-bits (256-bit AES + 1024-bit HMAC)	256-bits	768-bits (256-bit AES + 512-bit HMAC)

Select a Crypto Mode to match your network requirements. If you have a network of only older hardware "256-bit AES-CTR with HMAC-SHA-1" is the only option. If you have a network with a mix of older and newer hardware you should select the "Backwards Compatible: 256-bit AES-CTR with HMAC-SHA-1" mode on the units with newer hardware; this will allow all the nodes in the network to communicate. If you have a network with only newer hardware you can select any of the three modes. We recommend "256-bit AES-CTR with HMAC-SHA-512" as the mode with the greatest security margin. "256-bit AES-GCM" is an alternate full Suite-B mode that can also be used if the user prefers.

Once the Crypto Mode is set, enter a key value into the field and select "Set" or select "Generate" to generate a random key. The new key information is stored to the node or the network.

ZEROIZE

A key can be zeroized by pressing the pushbutton three times in quick succession or by using the Zeroize box under the "Security" tab.

The Zeroize box enables users to erase key configuration on an individual node or on the entire network as specified by the Node List. When a node is zeroized, all traces of the current key are erased so that it can no longer be recovered from the unit. Once a node has been zeroized, it cannot participate in any Wave Relay network until it is re-keyed using "Set Key".

When erasing security configuration, choose whether to Update the node only or the entire network. Changes to the network may require all nodes to be accessible so that security configuration is only erased if all nodes in the Node List can be contacted. In order to require all nodes in the Node List zeroize key configuration at the same time, select "Network - require all" from the Update pull-down menu. Otherwise, select "Network - any available", a function that zeroizes security configuration to only accessible nodes in the Node List.

The "Zeroize Key" button will erase just the packet encryption key. The "Zeroize All Configuration" button will additionally erase not only the key but also the management password and the public/private key-pair used to connect to the web management interface. If "all configuration" is selected, the node(s) will also reboot. When re-connecting to the management interface of a node that has been zeroized "all", the user will need to accept a newly generated certificate and use the factory password to authenticate.

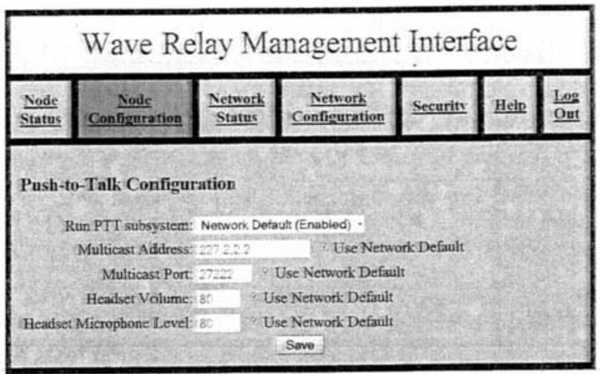


FIGURE 24: Push-to-Talk Configuration

Push-to-Talk (PTT) voice is supported on Wave Relay nodes that have a 6-pin NATO standard connector. Push-to-talk consists of a UDP data stream of G.711 encoded audio. The UPD data stream is multicast, enabling a walkie-talkie style communication system. In addition to providing voice communication among Wave Relay radios, the system can also incorporate Twisted Pair Solutions WAVE product family. By creating a channel in the WAVE system, which is configured to use the same multicast IP address, port, and G.711 codec, the two systems can interoperate, creating a large Radio over IP (RoIP) system.

To enable and configure push-to-talk, select "Push-to-Talk Configuration" from the Node Configuration Menu. Select "Enabled" under the "Run PTT subsystem" to turn push-to-talk on. Nodes that are to communicate using push-to-talk need to be on the same Multicast Address and Multicast Port. If two or more push-to-talk groups are going to exist at the same time, it is more efficient for them to have different Multicast Addresses. (see Figure 24: Push-to-Talk Configuration)

By default, Wave Relay supports single-channel PTT voice on a specified multicast IP address and port. You can "switch channels" by specifying an alternate IP address or port. Users can talk or listen (but cannot do both simultaneously). Transmissions from an individual user are broadcast to all other users on the network. Only one person can talk at a time.

MULTICHANNEL FEATURE

Wave Relay also supports multichannel voice. In this case, up to sixteen "talk groups" (numbered 0 through 15) can be configured on a network-wide basis, and individual users can listen to one or more groups (the default is to listen to all groups). When listening, only one channel may be heard at a time and thus the groups are prioritized with the lower-numbered groups having higher priority (e.g. traffic on group 3 will override all traffic on groups 4 through 15, and traffic on group 0 will override all other groups). An individual may transmit on one talk group at a time (though multiple users may be transmitting simultaneously on multiple groups).

The choice of single-channel or multichannel audio mode is determined on a network-wide basis and is configured in the Network Configuration screen.

For users of the Silynx C4OPS control module with a Wave Relay adapter cable, additional features supported on this headset include:

- Transmit group selection via the channel keys on the Silynx C4OPS
- Replay of the last received message via the hot key on the Silynx C4OPS

AUDIBLE NOTIFICATION FEATURE

The Audible Notification feature allows users to monitor the "in-network" and "out-of-network" status of any single node in the network. This is typically useful when a critical node drifts in and out of range and users want to be notified audibly when it becomes available/unavailable.

CONFIGURABLE FIELDS

Run PTT subsystem: Allows users to enable/disable push-to-talk audio.

Headset Volume: Valid values are 0 through 100. Optimal values vary with headset manufacturer.

Headset Microphone Level: Valid values are 0 through 100. Optimal values vary with headset manufacturer.

SINGLE TALK GROUP FIELDS

These fields are visible only when the network is in single-group mode.

Multicast Address: IP address for audio traffic. Must be within the range of 224.0.0.0 through 239.255.255.255. Note that all nodes within the talk group must be configured with the same address.

Multicast Port: UDP port for audio traffic. Must be within the range of 1 through 65534. Note that all nodes within the talk group must be configured with the same port.

MULTIPLE TALK GROUP FIELDS

These fields are visible only when the network is in multiple group mode. The list of available groups is displayed, allowing selection of which group(s) to receive. In addition, a single group may be selected for transmit. For users using the Silynx C4OPS control module, the selected transmit group can also be changed via the channel keys on the Silynx C4OPS.

AUDIBLE NOTIFICATION OF IN-NET/OUT-NET

This feature provides an audible notification when a tracked node becomes available for voice communication.

Audible Notification Mode: Enable/disable audible notification of the connectivity of a tracked node.

Node to Monitor: Select node to monitor when audible notification is enabled.

The RS-232 serial-over-Ethernet feature can be used for remote control of a distant serial device via the Wave Relay network. A typical application would be for a PC to control a pan-tilt camera via a serial link. If the PC and camera cannot be colocated, then two Wave Relays can be used to connect the devices (similar to an old-fashioned modem-to-modem link). Thus, the serial port on the PC can be hardwired to a local Wave Relay and the serial port on the camera can be hardwired to a distant Wave Relay. Communication between the two devices is then relayed via the Wave Relay network. This is called "serial-to-serial mode."

Alternatively, the PC can run emulation software which allows it to create a local virtual COM port which is configured to communicate directly with a distant network-enabled serial port (e.g. as described in RFC 2217). Thus, the camera is hardwired to a distant Wave Relay and the local PC can then connect directly to the distant device via Ethernet. This is called "virtual-to-serial mode."

To change RS-232 settings, go to "Node Configuration - RS-232 Configuration."

CONFIGURING SERIAL-TO-SERIAL MODE

Connect the serial device to be controlled (e.g. pan-tilt unit) to the serial port on the distant Wave Relay. Configure the RS-232 Configuration mode on the distant Wave Relay to "Server" and set the TCP port as desired (or leave as default). Set the protocol to "Raw." Set the serial port parameters to match those of the serial device (factory defaults for the Wave Relay are 57600 8-N-1 with no flow control). Click "Save" to store the settings.

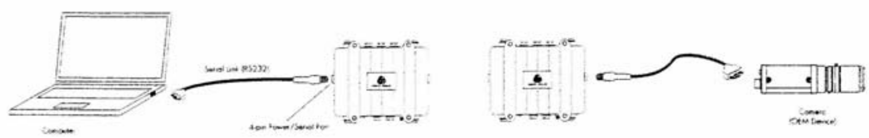
Connect the local serial device (e.g. PC) to the serial port on the local Wave Relay. Set the RS-232 Configuration mode on the local Wave Relay to "Client" and set the IP address and port to be those of the distant Wave Relay configured in step 1 above. Set the serial parameters to be identical to the distant device. Click "Save" to store the settings.

CONFIGURING VIRTUAL-TO-SERIAL MODE

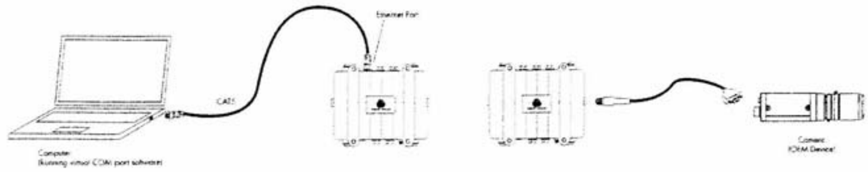
Connect and configure the serial device to be controlled (e.g. pan-tilt unit) as per step 1 above for Serial-to-Serial mode. For the Serial-over-Ethernet protocol, use whichever protocol is supported by your virtual client ("Raw" or "Telnet RFC 2217").

Install Virtual COM port software on the local PC (Eltima Serial to Ethernet Connector v5.0 for Windows has been tested and is known to work). Configure the virtual COM port to connect to the distant serial port via the address/port configured in step 1.

SERIAL-TO-SERIAL MODE



VIRTUAL-TO-SERIAL MODE



Go to "Node Configuration - Node Configuration."

Wave Relay over IP (WRoIP):

WRoIP allows the Wave Relay network to extend over and seamlessly interact with a large routed IP network. In order to use this capability, one or more Wave Relay nodes must be setup as WRoIP gateways. A WRoIP gateway must be directly connected to an appropriately configured IP router.

WRoIP: WRoIP gateway nodes must have the WRoIP protocol enabled on the interface directly connected to the IP router. All other nodes should have the WRoIP protocol disabled. When the WRoIP protocol is enabled on an interface, the interface will no longer function as a normal Wave Relay Ethernet port for connecting Ethernet devices: it will only work for connecting the IP router.

IP Address: The IP address of the WRoIP gateway in the IP subnet specific to the directly connected IP router interface. WRoIP protocol packets will be sent over the IP network using this IP address.

Netmask: The netmask of the IP subnet specific to the directly connected IP router interface.

Gateway: The IP address of the IP router in the IP subnet specific to the directly connected IP router interface. WRoIP protocol packets will be forwarded to this IP address in order to be sent over the IP network.

MTU: Maximum transmissible unit size for IP network. WRoIP protocol packets sent over the IP network will be limited to this MTU. All nodes that communicate over the IP network should be set to the same value.

Multicast Address: Multicast IP address used by the WRoIP protocol. The next higher IP multicast address will also be used by the WRoIP protocol. For example set 239.255.90.67 and both 239.255.90.67 and 239.255.90.68 will be used.

UDP Port: The UDP port used by WRoIP protocol packets.

NODE NAME: Nodes can be assigned a name such as "Wave Relay – 100". This name is used in management status functions.

IP ADDRESS: The IP address is required only for management and configuration functions. It is not required not for actual network operation.

NETMASK: Default netmask for the management interface.

GATEWAY: Default gateway for the management interface.

SNMP COMMUNITY STRING: Controls network SNMP access.

CHANNEL: Each radio must be assigned a channel frequency on which to operate. When the channel is configured to a Network Default, it can be managed globally through Network Configuration.

TRANSMIT POWER: A setting that controls the true output power including amplification offset, which can vary between radio modules. The setting affects both Access Point and Mesh communication. The setting is radio-specific. In general, this configuration is used only to reduce the output power of a radio for regulatory compliance reasons. The factory default should provide the best communication performance (highest power) in all other situations.

LINK DISTANCE: A setting that controls the ACK and SLOT TIMES for the MAC Controller. In order to setup a long-distance link, Link Distance needs to be configured properly. The Link Distance should be set to the maximum distance between any two nodes in the network. In general, increasing Link Distance results in moderately decreased system performance. Do not unnecessarily increase Link Distance well beyond what is required. All nodes on the same channel must use the same Link Distance setting. In point-to-point configuration, both links should have the same Link Distance. In point-to-multi-point configuration, all nodes, including the base station and subscriber stations, should have the same Link Distance even if some subscribers are closer to the base station than others. In mesh configuration, all of the mesh nodes on a given channel should have the same Link Distance.

MESH ROUTING: A radio-specific setting that determines whether a radio participates in the multi-hop mesh routing process. For example, for a multi-radio node for which the user wants the mesh running only on backhaul radios, this setting enables the user to disable the mesh on client access radios. Note that if a node is accessible only via the mesh and Mesh Routing is disabled for that node, then connection to that node will be lost.

MESH BROADCAST RATE: A setting for the broadcast rate of the mesh protocol coordination and discovery process. If the broadcast rate is too high, the system might be unreliable. In most cases, Mesh Broadcast Rate should be set to 11 Mbps (on 2.3 – 2.5 GHz radios) and lowered only if range over performance is preferred. If a radio that supports only OFDM (e.g. 5 GHz radios) is set to a non-OFDM Mesh Broadcast Rate, then the system will default to 6 Mbps. Increasing Mesh Broadcast Rate beyond the Factory Default will not increase network performance; it will serve only to reduce the effective range.

RADIO PREFERENCE: A setting that instructs the routing protocol to prefer links on a radio (i.e. to consider them lower cost than normal). This can be used to help to shift traffic towards radios running on certain channels.

NONE: The normal factory setting. All links are considered equally with the routing protocol's native metric.

MEDIUM: Medium bias towards links formed on this radio. Routing protocol is more likely to use this radio to forward traffic.

HIGH: High bias towards links formed on this radio. Routing protocol is significantly more likely to use this radio to forward traffic.

CONTENTION: A setting that controls how aggressively a radio competes for access to the shared medium. Contention directly affects the CSMA/CA Medium Access Control process. If a radio is configured as part of a Point to Point link with only two stations competing for access to the channel, then setting Contention to "Short" makes the radio highly aggressive and increases link performance. Contention can also be increased if the density of the mesh network is low. However, setting Contention to be more aggressive in higher density networks will adversely affect system performance.

ROOT GATEWAY PRIORITY: The Default Root Gateway Priority should generally be set to MEDIUM and then overridden on nodes which are connected to the wired infrastructure.

HIGH: Typically any node in your network which is directly connected to your wired infrastructure should have their priority set to "HIGH".

MEDIUM: All other non-mobile routers should be set to "MEDIUM".

LOW: Any mobile routers should be set to "LOW" priority.

DHCP SERVER FILTER: The network default for the DHCP server filter should generally be set to "BLOCK" and then overridden specifically on nodes which are directly connected to the wired infrastructure where the DHCP server is located. The factory default is "ALLOW" to facilitate out of the box configuration.

ALLOW: The DHCP Server Filter dictates which devices are allowed to bridge a DHCP server. In typical configurations it is desirable to have only a single DHCP server running on a given Ethernet segment. If the device is set to "ALLOW" it will pass DHCP messages from a DHCP server that is bridged directly by one of its interfaces. Only the devices that are wired directly to the switch where the DHCP server resides need to be set to "ALLOW".

BLOCK: If a device is set to "BLOCK" it will not bridge any DHCP reply packets that it picks up from its bridge interfaces. Setting all the nodes in the network (except the nodes on the wire with the real DHCP server) to "BLOCK" ensures that users will use the correct DHCP server. Doing so prevents users from incorrectly connecting client CPE devices to the system that responds to DHCP requests and other misconfiguration issues. It provides an added layer of security and system reliability.

802.11 ACCESS POINT: Each radio can be configured to function simultaneously as an 802.11 access point. This allows standard clients with built in 802.11 cards such as laptops to access the system. If the Access Point is disabled, the ESSID and Beacon Interval have no effect. In order to operate the radio as a standard 802.11 access point, it must be configured to operate on a 20 MHz channel width.

ESSID: The name of the network that the access point advertises to clients.

ESSID VISIBILITY: The ESSID can be advertised or not advertised. Generally, the ESSID is advertised to make it easy for clients to connect to the access point. For additional security/privacy the ESSID can be "HIDDEN".

AP BROADCAST RATE: A setting that controls the rate at which broadcasts are transmitted from the 802.11 access point. Increasing this rate can increase significantly network capacity but will reduce the range of client connectivity. If the rate is set too high, client devices will have trouble receiving broadcast packets from the 802.11 access point.

AP BEACON INTERVAL: The 802.11 access point can send beacons at an interval between two and ten times per second. The beacon interval should be set to ten times per second if you are running WPA or WPA2 security on the access point.

ROUTING METRIC: This setting allows the user to specify the link capacity to the routing protocol. A value lower than 100 Mbps (the default) should be used when nodes are connected via non-switched Ethernet (e.g. a third-party point-to-point wireless link). The setting allows the routing protocol to make an intelligent decision whether it is best to route over the Ethernet port or to use an alternate route that is faster.

VLAN ID: Each VLAN-aware bridge port is assigned a VLAN ID (a.k.a. Port VLAN Identifier, PVID, or Native VLAN). Untagged frames received by the port are tagged with the specified VLAN ID. Frames that are sent by the port that have a VLAN tag matching the specified VLAN ID will have their tags removed (i.e. they are sent by the port untagged).

All management features including the web interface, network visualization, SNMP, etc. run on a "virtual" internal management LAN-aware bridge port. This setting configures this node's management port VLAN ID (a.k.a. Port VLAN Identifier, PVID, or Native VLAN). The management port functions as an access port (no trunking), so the management features will only be accessible to the specified VLAN (traffic to/from all other VLANs is blocked/filtered). Take care when configuring the Ethernet/AP ports to disable trunking and use a VLAN ID different then the management port VLAN ID; the web management interface will be INACCESSIBLE to devices connected to these ports. Under these conditions, the web management interface is still accessible via another node with an Ethernet/AP port set to the same VLAN ID as this node's management port.

VLAN PRIORITY: This setting specifies the 802.1p priority of the VLAN tag added to untagged frames received by this port.

VLAN TRUNKING: A setting that controls the filtering of VLAN tagged frames that do NOT match the port VLAN ID. When trunking is enabled (trunk port), ALL non-matching VLAN tagged frames are passed (no filtering). When trunking is disabled (access port), all non-matching VLAN tagged frames are blocked (filtered).

UPDATE INTERVAL: When the visualization is enabled, nodes report information back to the visualization server at fixed intervals. This setting controls how often they report. If the network contains mobile nodes, setting the update interval to a shorter value will result in smoother movement of the node in Google Earth. However, the shorter the update interval, the more bandwidth used by the data reporting process. This update interval is also used to control the rate at which Cursor-on-Target messages are sent.

REPORT TO VISUALIZATION SERVER: A setting to enable network visualization for all nodes set to use the Network Default (typically the whole network). For proper Tracking Antenna System configuration, ensure that Report to Visualization Server is enabled on nodes that are to be tracked. Sending visualization updates can be individually enabled or disabled on each node. Usually, all nodes are set to Network Default, allowing visualization to be turned on and off for the entire network at once via the Network Default configuration. Note that the selected server IP address is shown here, but that it is configured as part of the Network Default configuration.

VISUALIZATION SERVER: A setting that specifies the IP address to which nodes send Visualization updates. This may be either a multicast address [224.0.0.0,239.255.255.255] or the unicast address of a device running the visualization server. The factory default is a multicast address. When using multicast, each node sends visualization updates to the entire connected network. All nodes run a visualization server and receive updates from all other connected nodes. When using unicast, each node sends visualization updates to only the selected address. If the unicast address is the management IP address of a node, that node will run a visualization server to receive the updates. Visualization updates are sent from the management IP address, so the selected address must be reachable by all nodes with visualization enabled; it should be either in the same subnet or reachable through the default gateway. Multicast operation allows the most robust visualization for mobile networks because it provides true distributed operation with partitions and merges. Unicast operation requires all visualization users to be able to contact the selected server, but offers reduced network overhead for larger static networks.

VISUALIZATION REPORTING INTERVAL: When visualization is enabled, nodes report information to the visualization server at fixed intervals. This setting controls how frequently the nodes report. If the network contains mobile nodes, setting the update interval to a smaller value will result in a smoother movement of the icon in Google Earth. The shorter the update interval, the more bandwidth is used by the data reporting process.

USE INTERNAL GPS: A setting to control from where GPS position information originates. If the node has an integrated GPS module and that module is used for position information, then check Use Internal GPS. This option should not be checked on a device that does not have an integrated GPS module,. This option should not be checked if a suitable GPS antenna with satellite connectivity is not attached. This option should not be checked if an external GPS source is used and position information is sent to the node via an "Update GPS" utility.

LATITUDE: Manually set the node's latitude. If the position is not specified, visualization will not provide useful information. Typically, after a node is installed, its position can be determined using Google Earth. Enter the position information from Google Earth into the configuration boxes.

LONGITUDE: Manually set the node's longitude. If the position is not specified, visualization will not provide useful information. Typically, after a node is installed, its position can be determined using Google Earth. Enter the position information from Google Earth into the configuration boxes.

ALTITUDE: Manually set the node's altitude in Feet Above Sea-Level. If the position is not specified, visualization will not provide useful information. Typically, after a node is installed, its position can be determined using Google Earth. Enter the position information from Google Earth into the configuration boxes.

ICON: An icon can be selected which will be used to identify the node in Google Earth.

WAVE RELAY OVER IP (WROIP): WRoIP allows the Wave Relay network to extend over and seamlessly interact with a large routed IP network. In order to use this capability, one or more Wave Relay nodes must be setup as WRoIP gateways. A WRoIP gateway must be directly connected to an appropriately configured IP router.

WROIP: WRoIP gateway nodes must have the WRoIP protocol enabled on the interface directly connected to the IP router. All other nodes should have the WRoIP protocol disabled. When the WRoIP protocol is enabled on an interface, the interface will no longer function as a normal Wave Relay Ethernet port for connecting Ethernet devices: it will only work for connecting the IP router.

IP ADDRESS: The IP address of the WRoIP gateway in the IP subnet specific to the directly connected IP router interface. WRoIP protocol packets will be sent over the IP network using this IP address.

NETMASK: The netmask of the IP subnet specific to the directly connected IP router interface.

GATEWAY: The IP address of the IP router in the IP subnet specific to the directly connected IP router interface. WRoIP protocol packets will be forwarded to this IP address in order to be sent over the IP network.

MULTICAST ADDRESS: Multicast IP address used by the WRoIP protocol. The next higher IP multicast address will also be used by the WRoIP protocol. For example set 239.255.90.67 and both 239.255.90.67 and 239.255.90.68 will be used.

UDP PORT: The UDP port used by WRoIP protocol packets.

SSPG SA ID: Simple SA Packet Generator Situational Awareness Identifier must be numeric and unique for each node.

APPENDIX D. RAVEN RQ 11B DATA SHEET

Raven

Overview

Raven® RQ-11B is a lightweight Unmanned Aircraft System (UAS) designed for rapid deployment and high mobility for both military and commercial applications, requiring low-altitude intelligence, surveillance, and reconnaissance (ISR).

Raven is the most prolific small UAS deployed with the U.S. Armed Forces. The vehicle can be operated manually or programmed for autonomous operation, utilizing the system's advanced avionics and precise GPS navigation.

Optional Stabilized Gimbaled Payload

- EO and IR cameras with IR Illuminator
- Continuous pan with +10 to –90 degrees tilt

Features

- No Runways Required
- Small Size, Lightweight & Hand-Launched
- Autonomous Navigation & Autoland
- Rugged for Extended, Reliable Use in Harsh Environments
- Delivers Realtime Situational Awareness
- Increases Combat Effectiveness and Force Protection

DDL Features

- More Capacity/Frequency Deconfliction
- Enhanced Data and Video Security
- Ethernet Bridge
- UAV/UGV/UGS Relay

Specifications

Standard Payloads	Dual Forward and Side-Look EO Camera Nose, Electronic Pan-tilt-zoom with Stabilization, Forward and Side-Look IR Camera Nose (6.5 oz payloads)
Range	10 km
Endurance	60–90 minutes (Rechargeable Battery)
Speed	32–81 km/h, 17–44 knots
Operating Altitude (Typ.)	100–500 ft (30-152 m) AGL, 14,000 ft MSL max launch altitude
Wing Span	4.5 ft (1.4 m)
Length	3.0 ft (0.9 m)
Weight	4.2 lbs (1.9 kg)
GCS	Lightweight, Modular Components, Waterproof Softcase, Optional FalconView Moving Map and Mission Planning Laptop Interface, Digital Video Recorder and Frame Capture
Launch & Recovery Method	Hand-Launched, Deep Stall Landing

www.avinc.com/raven

AV aerovironment

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E. IPREF BASELINE AND AIRBORNE RELAY TEST THROUGHPUT RATE AVERAGES

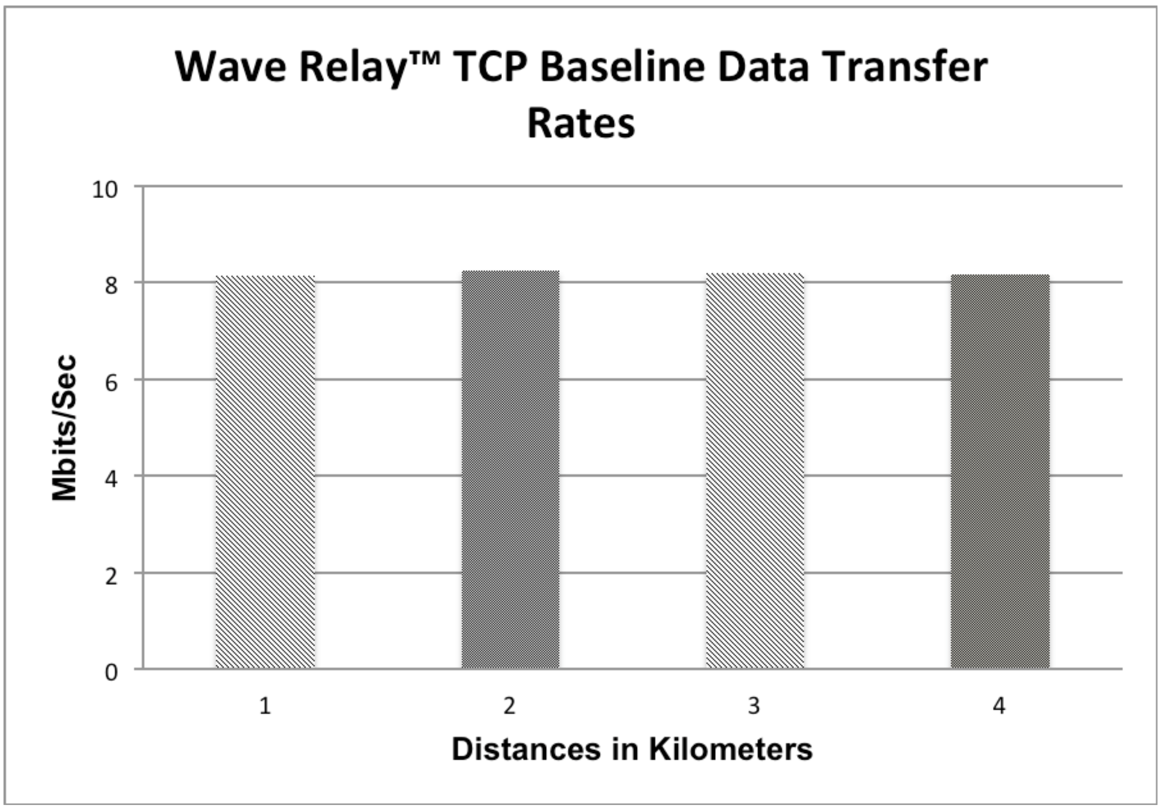
Ipref TCP Baseline Wave Rely™ Throughput Rates for distances 1-4km

Home | Layout | Tables | Charts | SmartArt | Formulas | Data | Review

D59

	A	B	C	D	E	F	G	H	I
1	TCP BANDWIDTH TRANSFER AVERAGES Mbits/Sec								
2		Distances	1Km	2Km	3Km	4Km		Environmental Test Conditions	
3		1	7.78	8.19	8.15	8.12		Day	Yes
4		2	7.8	8.22	8.17	8.13		Night	Yes
5		3	7.67	8.22	8.17	7.85		Clear	Yes
6		4	7.46	8.28	8.08	8.17		Winds	14-16 Kts
7		5	7.83	8.19	8.2	8.15			
8		6	7.8	8.22	8.26	8.16			
9		7	7.8	8.25	8.2	8.18		Samples/Dis	File Size Sample
10		8	7.84	8.28	8.2	8.16		50	10Mb
11		9	8.25	8.25	8.24	8.19			
12		10	8.22	8.26	8.23	8.2		Channel BW Setting	Packet Size
13		11	8.24	8.23	8.19	8.23		5MHz	1500kbit/Sec
14		12	8.07	8.29	8.21	8.12			
15		13	8.3	8.25	8.05	8.22			
16		14	8.25	8.22	8.13	8.2			
17		15	8.22	8.24	7.95	8.15			
18		16	8.28	8.31	7.92	8.17			
19		17	8.26	8.25	8.26	8.16			
20		18	8.29	8.24	8.18	8.19			
21		19	8.23	8.23	8.18	8.1			
22		20	8.22	8.26	8.23	8.24			
23		21	8.24	8.24	8.19	8.21			
24		22	8.28	8.28	8.19	8.2			
25		23	8.16	8.29	8.22	8.23			
26		24	8.23	8.27	8.19	8.19			
27		25	8.2	8.22	8.22	8.16			
28		26	8.22	8.24	8.23	8.18			
29		27	8.21	8.3	8.21	8.18			
30		28	8.3	8.28	8.24	8.2			
31		29	8.17	8.3	8.21	8.16			
32		30	8.29	8.24	8.23	8.15			
33		31	8.22	8.26	8.24	8.18			
34		32	8.23	8.19	8.18	8.22			
35		33	8.21	8.32	8.24	8.19			
36		34	8.25	8.32	8.25	8.21			
37		35	8.28	8.2	8.22	8.19			
38		36	8.29	8.24	8.15	8.21			
39		37	8.22	8.25	8.17	8.19			
40		38	8.23	8.21	8.24	8.21			
41		39	8.18	8.3	8.17	8.21			
42		40	8.24	8.27	8.25	8.16			
43		41	8.24	8.21	8.2	8.2			
44		42	8.29	8.27	8.22	8.2			
45		43	8.23	8.31	8.19	8.09			
46		44	8.24	8.26	8.24	8.13			
47		45	8.2	8.26	8.25	8.1			
48		46	8.22	8.26	8.22	8.2			
49		47	8.27	8.21	8.22	8.18			
50		48	8.24	8.21	8.19	8.17			
51		49	8.22	8.28	8.2	8.17			
52		50	8.24	8.26	8.18	8.25			
53		Average	8.157	8.2526	8.191	8.1722			
54		Standard Deviation	0.19	0.03	0.07	0.06			
55		Test Statistic							
56		P-Value							
57									
58									
59									
60									

TCP Data | UDP Data | AR TCP DATA | AR UDP Data | Combined TCP | Combined UDP | PTP


Wave Relay™ TCP Baseline Data Transfer Rates
10
8
6
4
2
0
Mbits/Sec
1
2
3
4
Distances in Kilometers

Ipref UDP Baseline Wave Rely™ Throughput Rates for distances 1-4km

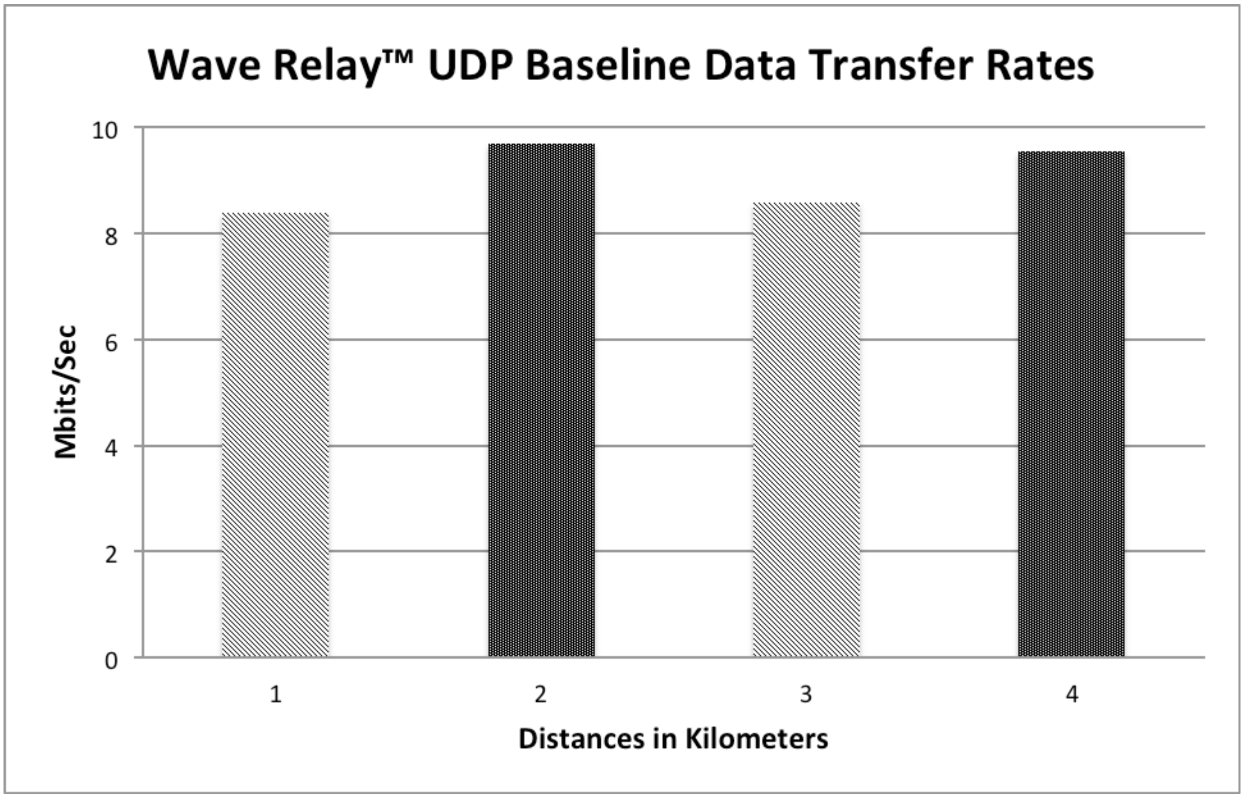
UDP DATA TRANSFER AVERAGES Mbits/Sec					
Distances		1Km	2Km	3Km	4Km
	1	9.29	9.92	7.21	9.76
	2	9.93	9.9	9.75	9.77
	3	9.93	9.9	9.87	9.71
	4	4.44	9.88	9.83	9.76
	5	3.07	9.86	9.89	9.84
	6	2.28	9.88	9.98	9.83
	7	9.98	9.89	9.86	9.83
	8	9.94	9.89	9.89	9.83
	9	9.94	9.89	9.99	9.83
	10	4.69	9.88	9.92	9.83
	11	9.93	9.92	9.88	9.85
	12	9.86	4.67	9.9	9.84
	13	9.72	9.9	9.96	9.83
	14	4.69	9.9	9.88	9.84
	15	3.08	9.87	9.67	9.84
	16	9.8	9.95	9.89	9.83
	17	9.95	9.9	9.95	9.86
	18	9.74	9.89	9.89	9.84
	19	9.9	9.9	9.88	9.84
	20	4.71	9.72	9.86	9.77
	21	9.98	9.88	9.85	9.82
	22	4.72	4.7	6.04	9.85
	23	3.09	9.89	8	9.84
	24	2.3	9.78	9.86	9.71
	25	1.82	9.92	8.51	9.6
	26	9.98	9.92	9.55	9.75
	27	9.94	9.9	9.75	4.62
	28	9.94	9.9	6.71	9.74
	29	4.69	9.89	6.18	9.81
	30	9.93	9.91	6.23	9.86
	31	9.93	9.89	6.19	9.85
	32	9.86	9.92	6.21	9.82
	33	9.98	9.91	6.19	9.77
	34	9.63	9.9	6.17	9.71
	35	9.99	9.89	6.19	9.74
	36	9.94	9.92	6.22	9.59
	37	9.87	9.92	6.08	9.4
	38	9.93	9.89	6.2	9.41
	39	9.93	9.9	6.06	9.62
	40	9.95	9.9	6.15	9.36
	41	9.91	9.93	6.22	9.7
	42	9.99	9.91	6.21	9.37
	43	9.94	9.94	9.71	9.72
	44	9.93	9.58	9.81	9.83
	45	9.64	9.91	9.85	9.81
	46	9.67	9.9	9.92	9.74
	47	9.84	9.91	9.89	9.72
	48	9.97	9.9	9.95	9.59
	49	9.94	9.93	9.8	4.55
	50	9.94	9.89	9.92	9.81
	Average	8.38	9.68	8.57	9.54
	Standard Deviation	2.75	1.03	1.71	1.03
	Test Statistic				
	P-Value				

Environmental Test Conditions	
Day	Yes
Night	Yes
Clear	Yes
Winds	14-16 Kts

Samples/Dis	File Size Sample
50	10Mb

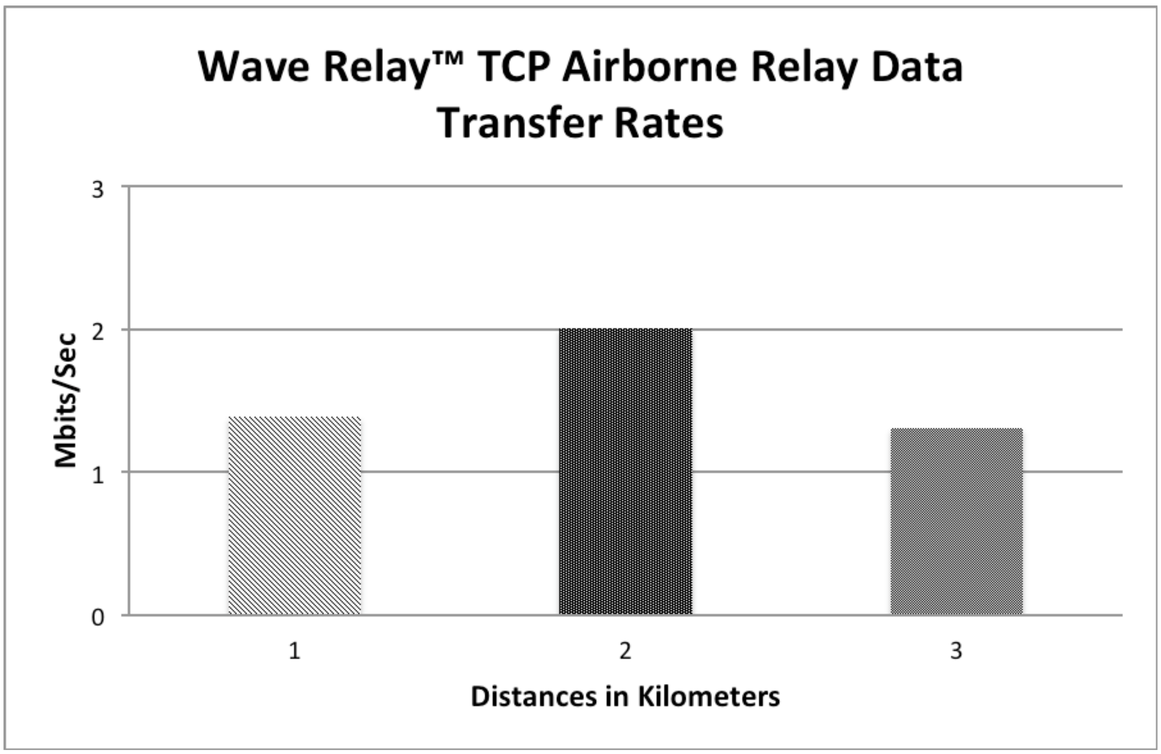
Channel BW Setting	Packet Size
5MHz	1500kbit/Sec

TCP Data | UDP Data | AR TCP DATA | AR UDP Data | Combined TCP | Combined UDP | PTP TCP_UDP CC


Wave Relay™ UDP Baseline Data Transfer Rates
Mbits/Sec
0
2
4
6
8
10
1
2
3
4
Distances in Kilometers

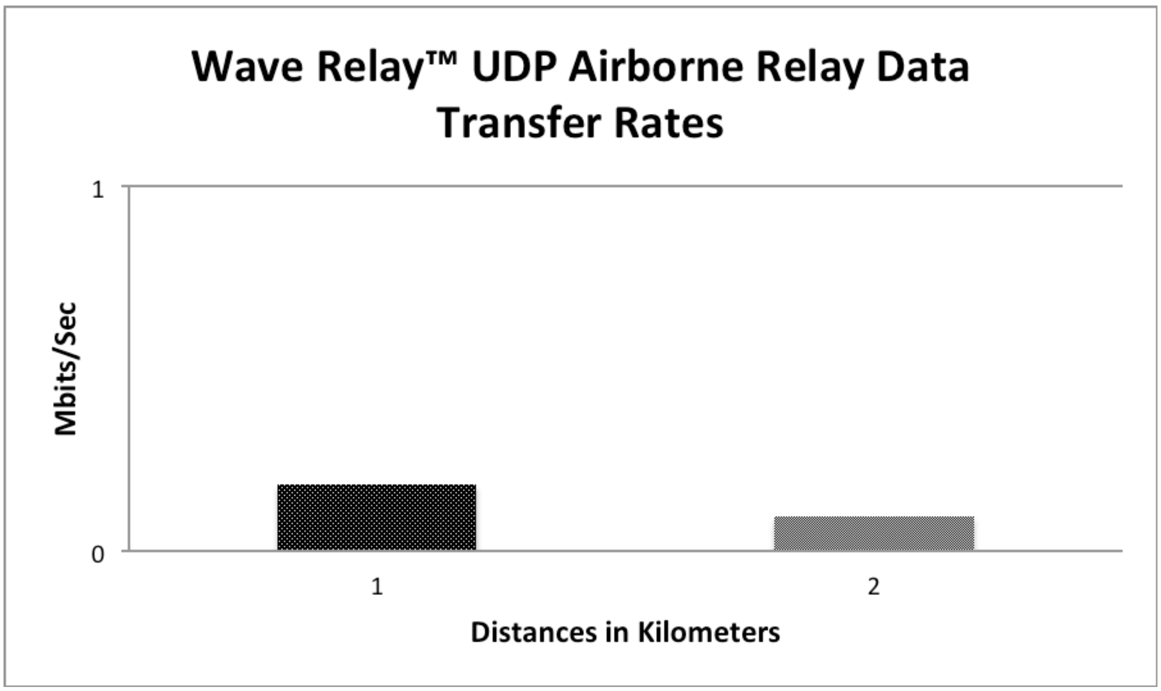
Ipref TCP Airborne Relay Wave Rely™ Throughput Rates for distances 1-3km

A	B	C	D	E	F	G	H
AR TCP BANDWIDTH TRANSFER AVERAGES Mbits/Sec							
	Distances	1Km	2Km	3Km		Environmental	Test Conditions
	1	1.2	2.2	0.46		Day	Yes
	2	2.29	3.13	1.1		Night	No
	3	1.43	1.43	1.27		Clear	Yes
	4	1.18	2.62	1.27		Winds	6Kts
	5	1.79	3.07	1.29			
	6	2.7	1.16	1.26			
	7	2.16	3.05	1.36		Samples/Dis	File Size Sample
	8	2.65	1.97	1.22		50	10Mb
	9	1.58	1.39	1.19			
	10	1.16	1.42	1.43		Channel BW Se	Packet Size
	11	1.36	1.82	0.26		5MHz	1500kbit/Sec
	12	1.55	2.81	1.43			
	13	1.64	0.77	1.66			
	14	1.44	2.53	1.17			
	15	1.6	0.87	1.99			
	16	1.55	1.5	1.24			
	17	1.51	2.99	2.1			
	18	1.61	2.17	1.21			
	19	1.58	1.15	1.78			
	20	1.26	2.73	0.93			
	21	1.73	1.1	1.89			
	22	2.34	3.01	1.13			
	23	2.48	2.52	1.61			
	24	1.69	1.99	1.07			
	25	1.55	1.47	1.72			
	26	1.72	2.55	1.18			
	27	1.37	1.09	1.65			
	28	1.59	3.13	1.11			
	29	1.69	1.97	1.31			
	30	1.41	1.17	1.21			
	31	0.59	2.54	1.59			
	32	0.67	0.93	1.94			
	33	1.37	2.81	1.12			
	34	1.21	1.07	1.83			
	35	0.99	3.14	1.09			
	36	1.3	1.84	1.66			
	37	0.96	1.41	0.84			
	38	1.05	2.82	1.12			
	39	1.03	0.88	1.51			
	40	0.6	2.81	1.02			
	41	1.14	1.52	1.79			
	42	0.66	1.73	1.02			
	43	0.43	2.66	1.73			
	44	0.79	0.98	1.1			
	45	0.8	3	1.59			
	46	0.76	1.45	0.86			
	47	0.99	1.69	1.02			
	48	0.61	2.01	1.2			
	49	1.35	1.18	0.87			
	50	1.34	2.91	0.86			
	Average	1.39	2.00	1.31			
	Standard Deviation	0.53	0.77	0.38			
	Test Statistic						
	P-Value						


Wave Relay™ TCP Airborne Relay Data Transfer Rates
3
2
1
0
Mbits/Sec
1
2
3
Distances in Kilometers

Ipref UDP Airborne Relay Wave Rely™ Throughput Rates for distances 1-2km

	A	B	C	D	E	F	G
1	AR UDP DATA TRANSFER AVERAGES Mbits/Sec						
2		Distances	1Km	2Km		Environmental Test Conditions	
3		1	1.48	0.52		Day	
4		2	1.18	0.76		Night	
5		3	1.49	0.46		Clear	
6		4	1.81	0.41		Winds	
7		5	0.54	0.27			
8		6	0.27	0.22			
9		7	0.25	0.15		Samples/Dis	File Size Sample
10		8	0.2	0.15		50	10Mb
11		9	0.12	0.11			
12		10	0.18	0.07		Channel BW Setting	Packet Size
13		11	0.23	0.06		5MHz	1500kbit/Sec
14		12	0.04	0.03			
15		13	0.04	0.04			
16		14	0.05	0.05			
17		15	0.06	0.03			
18		16	0.08	0.04			
19		17	0.04	0.07			
20		18	0.06	0.11			
21		19	0.06	0.09			
22		20	0.06	0.1			
23		21	0.06	0.05			
24		22	0.04	0.05			
25		23	0.05	0.04			
26		24	0.04	0.03			
27		25	0.03	0.01			
28		26	0.03	0.03			
29		27	0.02	0.02			
30		28	0.03	0.02			
31		29	0.02	0.05			
32		30	0.04	0.08			
33		31	0.03	0.06			
34		32	0.03	0.07			
35		33	0.02	0.05			
36		34	0.03	0.02			
37		35	0.03	0.01			
38		36	0.02	0.01			
39		37	0.03	0.01			
40		38	0.02	0.03			
41		39	0.02	0.04			
42		40	0.03	0.06			
43		41	0.03	0.04			
44		42	0.02	0.04			
45		43	0.03	0.03			
46		44	0.03	0.04			
47		45	0.02	0.02			
48		46	0.03	0.02			
49		47	0.02	0.01			
50		48	0.02	0.02			
51		49	0.02	0.02			
52		50	0.02	0.01			
53		Average	0.182	0.09			
54		Standard Deviation	0.41	0.15			
55		Test Statistic					
56		P-Value					



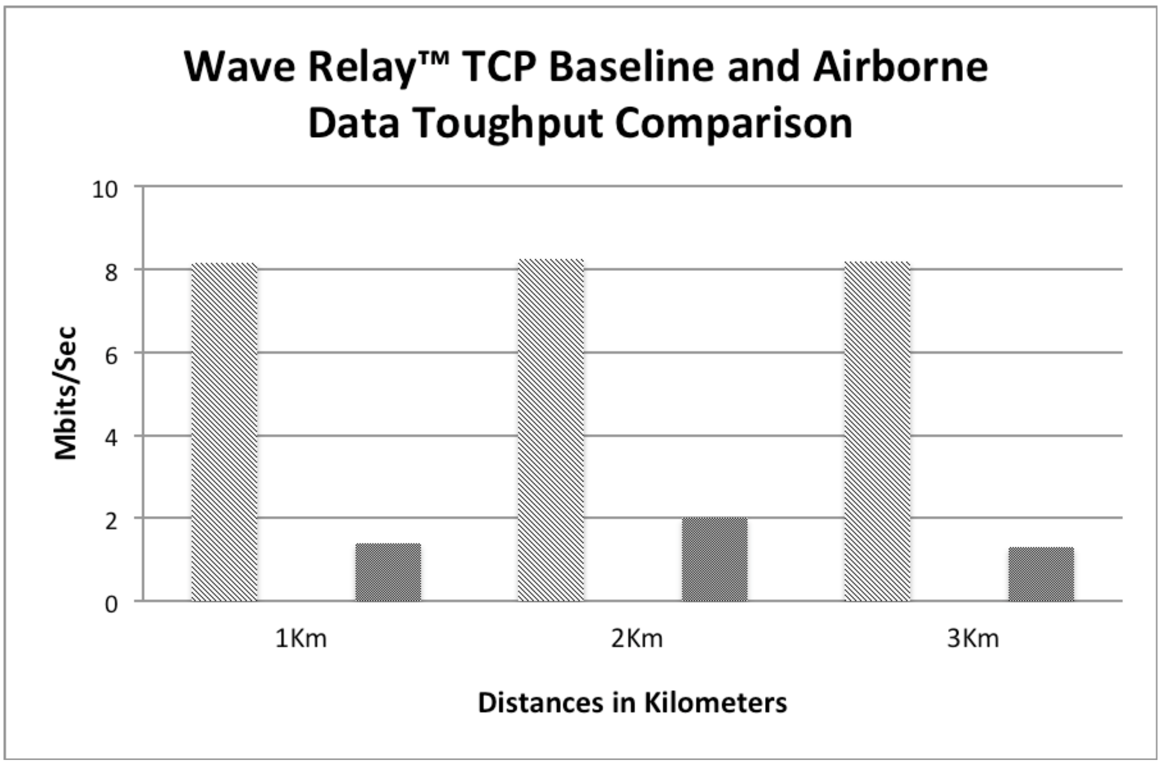
Wave Relay™ UDP Airborne Relay Data Transfer Rates
1
0
Mbits/Sec
1
2
Distances in Kilometers

Ipref Combined Baseline and Airborne Relay Wave Rely™ Throughput Rates for distances 1-3km

COMBINED TCP BANDWIDTH TRANSFER AVERAGES Mbits/Sec

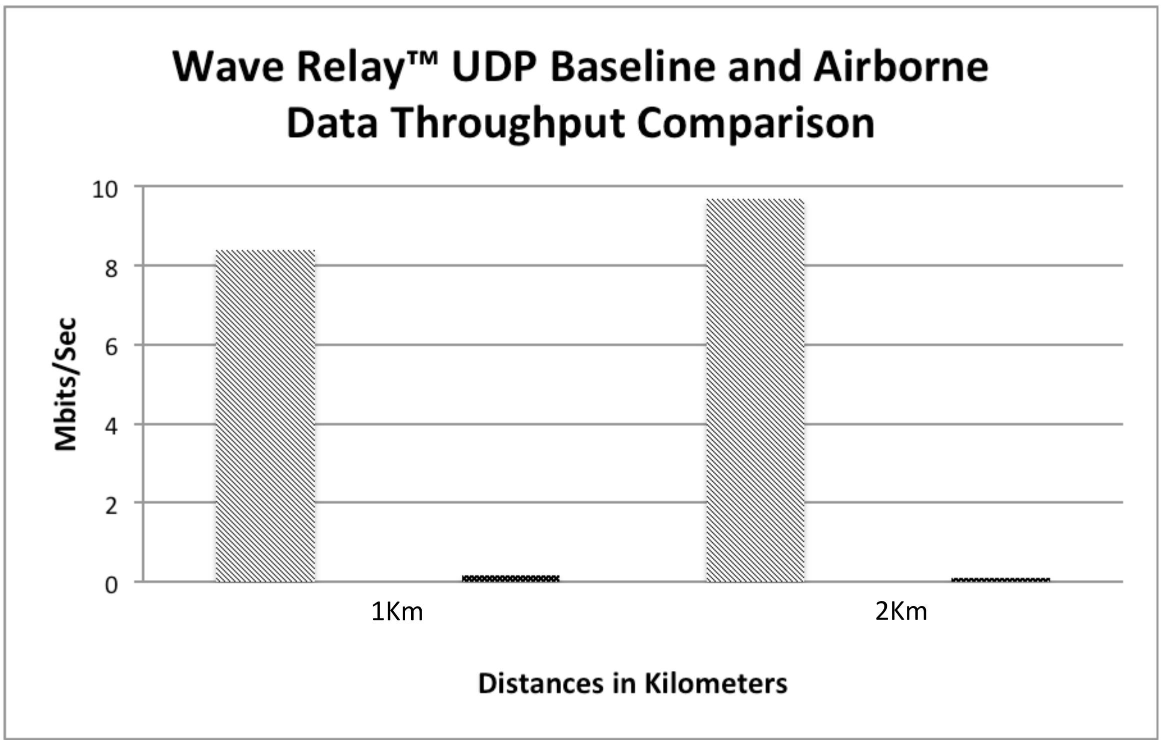
Distances	1Km		2Km		3Km	
	X	Y	X	Y	X	Y
1	7.78	1.2	8.19	2.2	8.15	0.46
2	7.8	2.29	8.22	3.13	8.17	1.1
3	7.67	1.43	8.22	1.43	8.17	1.27
4	7.46	1.18	8.28	2.62	8.08	1.27
5	7.83	1.79	8.19	3.07	8.2	1.29
6	7.8	2.7	8.22	1.16	8.26	1.26
7	7.8	2.16	8.25	3.05	8.2	1.36
8	7.84	2.65	8.28	1.97	8.2	1.22
9	8.25	1.58	8.25	1.39	8.24	1.19
10	8.22	1.16	8.26	1.42	8.23	1.43
11	8.24	1.36	8.23	1.82	8.19	0.26
12	8.07	1.55	8.29	2.81	8.21	1.43
13	8.3	1.64	8.25	0.77	8.05	1.66
14	8.25	1.44	8.22	2.53	8.13	1.17
15	8.22	1.6	8.24	0.87	7.95	1.99
16	8.28	1.55	8.31	1.5	7.92	1.24
17	8.26	1.51	8.25	2.99	8.26	2.1
18	8.29	1.61	8.24	2.17	8.18	1.21
19	8.23	1.58	8.23	1.15	8.18	1.78
20	8.22	1.26	8.26	2.73	8.23	0.93
21	8.24	1.73	8.24	1.1	8.19	1.89
22	8.28	2.34	8.28	3.01	8.19	1.13
23	8.16	2.48	8.29	2.52	8.22	1.61
24	8.23	1.69	8.27	1.99	8.19	1.07
25	8.2	1.55	8.22	1.47	8.22	1.72
26	8.22	1.72	8.24	2.55	8.23	1.18
27	8.21	1.37	8.3	1.09	8.21	1.65
28	8.3	1.59	8.28	3.13	8.24	1.11
29	8.17	1.69	8.3	1.97	8.21	1.31
30	8.29	1.41	8.24	1.17	8.23	1.21
31	8.22	0.59	8.26	2.54	8.24	1.59
32	8.23	0.67	8.19	0.93	8.18	1.94
33	8.21	1.37	8.32	2.81	8.24	1.12
34	8.25	1.21	8.32	1.07	8.25	1.83
35	8.28	0.99	8.2	3.14	8.22	1.09
36	8.29	1.3	8.24	1.84	8.15	1.66
37	8.22	0.96	8.25	1.41	8.17	0.84
38	8.23	1.05	8.21	2.82	8.24	1.12
39	8.18	1.03	8.3	0.88	8.17	1.51
40	8.24	0.6	8.27	2.81	8.25	1.02
41	8.24	1.14	8.21	1.52	8.2	1.79
42	8.29	0.66	8.27	1.73	8.22	1.02
43	8.23	0.43	8.31	2.66	8.19	1.73
44	8.24	0.79	8.26	0.98	8.24	1.1
45	8.2	0.8	8.26	3	8.25	1.59
46	8.22	0.76	8.26	1.45	8.22	0.86
47	8.27	0.99	8.21	1.69	8.22	1.02
48	8.24	0.61	8.21	2.01	8.19	1.2
49	8.22	1.35	8.28	1.18	8.2	0.87
50	8.24	1.34	8.26	2.91	8.18	0.86
Average	8.16	1.39	8.25	2.00	8.19	1.31
Standard Deviation	0.19	0.53	0.03	0.77	0.07	0.38
Test Statistic		85.17		57.06		174.38
P-Value		0.00		0.00		0.00

X= Point to Point
Y= Air Relay
N=50


Wave Relay™ TCP Baseline and Airborne
Data Toughput Comparison
10
8
6
4
2
0
Mbits/Sec
1Km
2Km
3Km
Distances in Kilometers

Ipref Combined Baseline and Airborne Relay Wave Rely™ Throughput Rates for distances 1-2km

	A	B	C	D	E	F	G	H
1	COMBINED UDP DATA TRANSFER AVERAGES Mbits/Sec							
2		Distances	1Km		2Km			
3			X	Y	X	Y		X= Point to Point
4		1	9.29	1.48	9.92	0.52		Y= Air Relay
5		2	9.93	1.18	9.9	0.76		N=50
6		3	9.93	1.49	9.9	0.46		
7		4	4.44	1.81	9.88	0.41		
8		5	3.07	0.54	9.86	0.27		
9		6	2.28	0.27	9.88	0.22		
10		7	9.98	0.25	9.89	0.15		
11		8	9.94	0.2	9.89	0.15		
12		9	9.94	0.12	9.89	0.11		
13		10	4.69	0.18	9.88	0.07		
14		11	9.93	0.23	9.92	0.06		
15		12	9.86	0.04	4.67	0.03		
16		13	9.72	0.04	9.9	0.04		
17		14	4.69	0.05	9.9	0.05		
18		15	3.08	0.06	9.87	0.03		
19		16	9.8	0.08	9.95	0.04		
20		17	9.95	0.04	9.9	0.07		
21		18	9.74	0.06	9.89	0.11		
22		19	9.9	0.06	9.9	0.09		
23		20	4.71	0.06	9.72	0.1		
24		21	9.98	0.06	9.88	0.05		
25		22	4.72	0.04	4.7	0.05		
26		23	3.09	0.05	9.89	0.04		
27		24	2.3	0.04	9.78	0.03		
28		25	1.82	0.03	9.92	0.01		
29		26	9.98	0.03	9.92	0.03		
30		27	9.94	0.02	9.9	0.02		
31		28	9.94	0.03	9.9	0.02		
32		29	4.69	0.02	9.89	0.05		
33		30	9.93	0.04	9.91	0.08		
34		31	9.93	0.03	9.89	0.06		
35		32	9.86	0.03	9.92	0.07		
36		33	9.98	0.02	9.91	0.05		
37		34	9.63	0.03	9.9	0.02		
38		35	9.99	0.03	9.89	0.01		
39		36	9.94	0.02	9.92	0.01		
40		37	9.87	0.03	9.92	0.01		
41		38	9.93	0.02	9.89	0.03		
42		39	9.93	0.02	9.9	0.04		
43		40	9.95	0.03	9.9	0.06		
44		41	9.91	0.03	9.93	0.04		
45		42	9.99	0.02	9.91	0.04		
46		43	9.94	0.03	9.94	0.03		
47		44	9.93	0.03	9.58	0.04		
48		45	9.64	0.02	9.91	0.02		
49		46	9.67	0.03	9.9	0.02		
50		47	9.84	0.02	9.91	0.01		
51		48	9.97	0.02	9.9	0.02		
52		49	9.94	0.02	9.93	0.02		
53		50	9.94	0.02	9.89	0.01		
54		Average	8.38	0.18	9.68	0.09		
55		Standard Deviation	2.75	0.41	1.03	0.15		
56		Test Statistic		20.85		65.05		
57		P-Value		0.00		0.00		


Wave Relay™ UDP Baseline and Airborne Data Throughput Comparison
10
8
6
4
2
0
Mbits/Sec
1Km
2Km
Distances in Kilometers

LIST OF REFERENCES

AeroViroment Inc. (n.d.). *UAS: Raven*. Retrieved from http://www.avinc.com/uas/small_uas/raven/

Antoine, J. (2012, May). Combat skysat. *MILSATMAGAZINE*, *3*(2), 11–13.

Austin, R. (2010). *Unmanned aircraft systems: UAVS design, development, and deployment.* Chichester, West Sussex, United Kingdom: John Wiley & Sons Ltd.

Barker, D. (2008, December 11). *New communication balloon capabilites tested aboard USS Boxer*. Retrieved from MILCOM Monitoring Post website: http://mt-milcom.blogspot.com/2008/12/new-communication-balloon-capabilites.html

Battlefield communications go wideband. (2008, August). *Frequency*.

Boutelle, S. W. (1996, Spring). AFATDS: The fire support window to the 21st century. *Joint Forces Quarterly*, *11*, 16–21.

Cebrowski, A. K. (1998, January). Network-centric warfare: Its orgin and future. *Proceedings*, 1–12.

Department of Defense. (2009). *FY2009–2034 unmanned systems integrated roadmap.* Washington, DC: Department of Defense.

Dombrowski, P. J., & Gholz, E. (2006). *Buying military transformation: Technological innovation and the defense industry*. New York, NY: Columbia University Press.

Edwards, J. (2012, April). Tactical radios and mobile devices: Powered by imagination. *Defense Systems*, 1–5.

Gilder, G. (1993, September 13). Metcalf's law and legacy. *Forbes ASAP*, 1–8.

Google Inc. (2012). Google Earth (Version 6.2) [Software].

Held, G. (2005). *Introduction to wireless mesh networking.* Auerbach Publications.

Information Sciences Institute. University of Southern Califronia. (n.d.a.). *User datagram protocol. RFC: 768*. Retrieved from Internet Engineering Task Force website: http://tools.ietf.org/html/rfc768

Information Sciences Institute. University of Southern Califronia. (n.d.b.). *Transmission control protocol. RFC: 793*. Retrieved from Internet Engineering Task Force website: http://www.ietf.org/rfc/rfc793.txt

Isherwood, M. (2008, February). The new generation of unmanned aircraft systems and the Marine Corps. *Marine Corps Gazette*, 13–15.

Jamison, L. S. (2005). *High-altitude airships for the future force Army*. RAND Arroyo Center. Santa Monica: RAND Corporation.

Jane's Information Group. (2009). *AN/VRC-99 communications system (United States), tactical communications*. Retrieved from http://articles.janes.com/articles/Janes-Military-Communications/AN-VRC-99-communications-system-United-States.html

KAMAN Products and Services. (n.d.). *Unmanned aerial systems*. Retrieved from http://www.kaman.com/aerospace/helicopters/products-services/unmanned-aerial-systems/

Keller, G. (2008). *Statistics for management and economics* (vol. 8). Mason, Ohio, USA: Cengage Learning.

Kurose, J. R. (2010). *Computer networking: A top down approach* (5th vol.). M. Hirsch, Ed. Boston, MA: Pearson Education.

Marine Corps Systems Command. (2011). *Programs & equipment fact book 2011*. USMC, Marine Corps Systems Command. Washington, DC: USMC.

Military.com. (n.d.). *Global broadcast system*. Retrieved from http://www.military.com/ContentFiles/techtv_update_global.htm

National Institute of Standards and Technology. Advanced Network Technologies Division Wireless Ad Hoc Networks. (n.d.). *Mobile ad hoc networks (MANETs)*. Retrieved from http://w3.antd.nist.gov/wahn_mahn.shtml

Persistent Systems. (n.d.). *Persistent systems wave relay®*. Retrieved from http://www.persistentsystems.com/technology.php

Richerson, J. P. (2007). *The extension of wireless mesh networks via vertical takeoff and landing unmanned aerial vehicles* (master's thesis). Naval Postrgraduate School, Monterey,CA.

Ryan, M. (2002). *Tactical Communications for the digitized battlefield*. Boston, MA: Artech House.

SourceForge. (n.d.). *Iperf*. Retrieved from http://iperf.sourceforge.net

Tate, T. K. (2003). *Dragon warrior communications relay testing using the K-MAX helicopter*. Naval Research Laboratory, Communication Systems Branch. Washington, DC: Naval Research Laboratory.

Tharp, D., & Wallace L. (2003). *Enhanced position location reporting system: Legacy system provides new technology for warfighters institution*. Retrieved from Spawar website: http://www.spawar.navy.mil/sti/publications/pubs/td/3155/5a_S4papers/EPLRS.pdf

Thunder Power RC. (n.d.). *G6 pro power 65C series lipo batteries*. Retrieved from http://thunderpowerrc.com/html/G6ProPower65CSeriesBatteries.htm

United States Marine Corps. (1998). *Organization of Marine Corps forces*. Marine Corps Logistics Base Albany, GA. Retrieved from http://www.marines.mil/news/publications/Documents/MCRP%205-12D%20Organization%20of%20Marine%20Corps%20Forces.pdf

United States Marine Corps. (2011). *U.S. Marine Corps conepts & programs 2011*. U.S. Marine Corps, PP&O. Washington, DC: U.S. Marine Corps.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr. Doug MacKinnon
   Naval Postgraduate School
   Monterey, California

4. Marine Corps Representative
   Naval Postgraduate School
   Monterey, California

5. Director, Training and Education, MCCDC, Code C46
   Quantico, Virginia

6. Director, Marine Corps Research Center, MCCDC, Code C40RC
   Quantico, Virginia

7. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
   Camp Pendleton, California

8. Marine Corps Systems Command PG-11
   Quantico, Virginia

9. I Marine Expeditionary Force (Attn: Communications Officer)
   Camp Pendleton, California

10. California Department of Forestry and Fire Protection (Attn: Communication Liaison)
    Shasta, California